|  |
| --- |
| 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.

|  |
| --- |
| Phishing Attack, Data Leakage/Compromised, Malware Infections |

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.)

|  |
| --- |
| Employees should be informed of the risk of accessing work on personal devices. However, if it cannot be avoided, atleast they are aware of possible breach and threats like emails or websites access. |

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.)

|  |
| --- |
| To measure how often employees are not behaving according to preferred behaviors, such as downloading email attachments from unknown senders, I can use a combination of quantitative and qualitative methods. My structured approach would be: 1. Surveys and Self-Reports **Method**: Conduct anonymous surveys or questionnaires to gather data on employee behaviors and attitudes.  **Questions to Include**:   * How often do you download email attachments from unknown senders? * Have you received training on recognizing phishing or malicious attachments? * How confident are you in identifying suspicious email content?   **Pros**: Provides direct insights into employee behaviors and perceptions. **Cons**: Relies on self-reporting, which may not always be accurate. \*\*2. Incident Tracking and Reporting **Method**: Track and analyze security incidents related to email attachments.   * **Data Points**:   + Number of reported incidents involving email attachments from unknown sources.   + Frequency of security breaches linked to email attachments.   + Types of incidents and their severity.   **Pros**: Provides concrete data on actual security events. **Cons**: Requires proper incident reporting mechanisms and may not capture all incidents. \*\*3. Monitoring and Analytics **Method**: Use email and network monitoring tools to analyze attachment downloads and interactions.   * **Metrics**:   + Frequency of downloads from unknown or suspicious sources.   + Patterns in email attachment downloads.   + Correlation with known phishing or malware attacks.   **Pros**: Offers real-time data and can identify trends or patterns.  **Cons**: May raise privacy concerns and requires appropriate monitoring tools. |

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.)

|  |
| --- |
| I would set a click rate of maximum 5%. Exceeding CR result will be seriously handled. |

### 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 relevant staff I would be discussing this plan would be:   1. CEO-Responsible for plotting overall direction, from planning toimplementation. In addition to set and approve the security goalswithin the organisation. 2. CISO-play the main role in looking for the implementation of securitymeasures and monitoring the compliance and security protocols. Theyare responsible for protecting the data, identifying threats and respondto threats. 3. HR Department-Responsible for implementing and developing thepolicies related to employee's behaviour during the implementationand maintaining of the security proposed by CISO team. They are alsoinvolved for organising trainingprograms. 4. CFO-Designated to provide outlook and guidance on financial aspectsduring the implementation. They will also ensure the budgetaryresources are properly allocated. 5. CIO-Implementation of technical solutions mitigating the risksassociated by employees who use their personal devices to accesswork webs or emails |

### 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)?

|  |
| --- |
| **Hybrid:**  A face-to-face training/seminar discussing awareness of security measures.  A combination of both should apply to the trainingand a quarterly meeting ifthe same issue arise and to monitor the employees compliance is maintained. |

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

|  |
| --- |
| Important points I would include will be:   1. Security awareness training including risks of Personal device usage to discusspotential threats related to access of work data using personal devices, includingbreaches and malware infection. 2. Safe email Practices-to discuss how to identify and how respond phishing emailattacks. 3. Importance of Reporting Security Incidents- Educate them the importance of reporting suspected cyber attacks. Impose the seriousness of Incident Report. |

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

|  |
| --- |
| Conduct post-training surveys by gathering feedbacks with questions related to the training topics to evaluate that the employees understand the risks, threats and response. |

### 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?

|  |
| --- |
| 1. Mobile device management (MDM)-is a type of technical control.   Goal: Preventive and detective   * Advantage: To permit organisations to impose security policies on mobile devicessuch as encryption requirement and restricting downloads of unauthorisedapps.   Disadvantage: It requires additional resources and infrastructure to manageeffectively. |
|  |

|  |
| --- |
| 1. Endpoint Detection and Response   Goal: Detective and Corrective   * Advantage: to monitor end points (Laptops) for malicious or suspiciousbehaviour and also provides important insights to provide the cause of theincidents.   Disadvantage: False positive detection of threats due to high sensitivity tothreats. |

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