WEEK 2 :

**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.

|  |
| --- |
| When employees are allowed to access work information on their personal devices, they may store sensitive data on their personal devices without adequate security measures, putting sensitive corporate data at risk. Three potential attacks that can be carried out would be main-in-the-middle that can intercept communication between the employee’s device and the corporate. Another attack would be malware infection that can compromise the security of both personal and work-related data stored on the device. Phishing can also be carried out, compromising data, stealing login credentials. |

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 access work information only through secure networks such as trusted Wi-Fi networks with encryption. Employees should follow the organization’s policies and guidelines regarding the use of personal devices for work purposes. |

1. What methods would you use to measure how often employees are currently *not* behaving according to their preferred behavior? (For example, conduct a survey to see how often people download email attachments from unknown senders.)

|  |
| --- |
| Implement Mobile Device Management solutions that allow IT administrators to monitor and manage personal devices accessing corporate data and provide insights into devices configurations and security patterns. |

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.)

|  |
| --- |
| Educate employees about the potential security risks associated with using personal devices for work related activities. Emphasize the importance of protecting sensitive corporate information from unauthorized access, data breaches, and malware infections. |

**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) **IT Security Department**: They should educate employees about the risks associated with using personal devices and provide guidelines on how to mitigate the risks.  2) **Human Resources Department**: Create a clear policy outlining the acceptable use of personal devices for work purposes. This policy should detail expectations, responsibilities, security measures, and consequences for non-compliance, ensuring that all employees are aware of and understand the policy.  3)  **Information Technology.** Develop a BYOD policy that outlines the acceptable use of personal devices for work and defines security requirements, such as device encryption and passcode protection. Ensuring that employees acknowledge and agree to abide by the policy before accessing corporate resources on their personal devices.  4) **Legal and Compliance Department**: Require employees to sign consent forms or acknowledgment agreements indicating their understanding of an agreement to comply with the policies governing personal device usage. This documentation serves as evidence of employees' acknowledgment of their responsibilities.  5) **Employee Training Department**: Offer training sessions to educate employees on how to securely use their personal devices for work. This training should cover topics such as data security, password management, encryption, and the importance of keeping devices up to date. |

**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)?

|  |
| --- |
| Offering quarterly sessions to reinforce key security awareness messages and provide updates on emerging threats or changes to security policies and procedures. These shorter sessions can focus on specific topics or recent security incidents relevant to the organization. Online training can easily be scaled to accommodate many participants, making it suitable for organizations of all sizes. |

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

|  |
| --- |
| In the training, it is crucial to cover a range of topics to ensure that employees are well-informed about potential threats and best practices for mitigating risks. Some essential topics to include in the training and why they are important would be as follows.  **-Phishing Awareness:** Phishing attacks are one of the most common and effective methods used by cybercriminals to trick employees into revealing sensitive information or downloading malware. Training in phishing awareness educates employees on how to recognize phishing emails, suspicious links, and other social engineering tactics, helping to reduce the risk of falling victim to these attacks.  **-Device Security**: Mobile devices and laptops are common targets for cyberattacks, especially in environments where employees use personal devices for work purposes. Training on device security educates employees on how to secure their devices with strong passwords, enable encryption, install security updates, and use remote wipe or lock features to protect sensitive data in case of loss or theft.  **-Password Security**: Weak or compromised passwords are a significant security risk for organizations. Training on password security covers best practices for creating strong, unique passwords and guidelines for securely storing and managing passwords. This helps prevent unauthorized access to sensitive systems and accounts.  **-Incident Response Procedures**: Despite preventive measures, security incidents may still occur. Training on incident response procedures equips employees with the knowledge and skills to recognize, report, and respond to security incidents effectively such as containing the incident, notifying appropriate personnel, preserving evidence, and cooperating with incident response teams. |

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

|  |
| --- |
| After the training, it is essential to ensure that employees have gained the knowledge and skills needed to mitigate security threats effectively. Conduct practical exercises and simulations activities to assess employees' proficiency in recognizing and responding to security threats. Ask participants to provide feedback on the relevance of the training topics. |

**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?

|  |
| --- |
| Multi Factor Authenticationadds an extra layer of security by requiring users to provide multiple forms of authentication, such as a password and a unique code sent to their mobile device before gaining access to sensitive data. The type of control is technical, and the goal of control is preventive and detective. One advantage would be to add an extra layer of security by requiring users to provide multiple forms of authentication such as a unique code sent to their mobile devices. One disadvantage would be that some users may find MFA processes time consuming and too many authentication factors are required leading to frustration and decreased productivity. |

|  |
| --- |
| Security Awareness Training is another potential solution, the control is administrative and the goal of control of this training is preventive, deterrent, and detective. Iteducates employees about common security threats, such as phishing attacks, malware, and social engineering tactics, empowering them to recognize and avoid potential risks. |