| Cybersecurity |
| --- |
| Module 2 Challenge Submission File |

## Assessing Security Culture

### Step 1: Measure and Set Goals

1. Using outside research indicates the potential security risks of allowing employees to access work information on their devices. Identify at least three potential attacks that can be carried out.

| Potential attacks could be: 1. Data theft  2. Man-in-the-middle attacks 3. Phishing attacks |
| --- |

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 would be that employees avoid the usage of personal devices and public networks to login and access work-related information. |
| --- |

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.)

| By analyzing the firewall log activity to track unauthorized devices being used to access work networks <https://www.manageengine.com/products/firewall/images/fwa-traffic-statistics.png> |
| --- |

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.)

| To reduce from 25% of employees using personal devices for work-related activities to 5%. 0%(if possible) |
| --- |

### 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. Learning and Development(L&D)- This department is in charge of onboarding employees and going through the basic training needed to understand some of the risks in cybersecurity. 2. Enterprise risk management(ERM)- This department will further train and prepare the staff in risk assessment. It will also provide different levels of data access based on employees' roles. 3. Team leaders- These are the first filters in which information will be passed through, and will also be there for support and guidance against adversity. 4. Managers- Managers will overview the work of the Team leads as well as the entire team, assessing and reinforcing company safety policies and desired outcomes. 5. Soc analysts- is a 24-hour control center in charge of security and threat analysis for an organization. SOC definition is taken from: <https://www.freelancermap.com/blog/what-does-soc-analyst-do/> |
| --- |

### Step 3: Training Plan

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

| In an industry that is ever-changing and evolving, training will be implemented half yearly with a combination of both in-person and online, to optimize involvement and full understanding of the topic. Following with exercises to ensure the effectiveness of training. |
| --- |

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

| This training will be based on the potential threats of allowing employees to access work information on their personal devices. So it will cover topics such as :   1. What is phishing? 2. Phishing prevention 3. How to identify risks and threats 4. Passwords management 5. Identity theft 6. Social engineering and how it happens |
| --- |

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

| Some methods to ensure effectiveness in the training would be: 1. Screen monitoring: This will allow us to track in real-time the activity and URLs being opened by staff members. Could help us see which employees are failing to follow protocol.  2. Have a department run a basic form of pen testing, which could expose the employees to phishing emails and to other ways of how data can be compromised.  3. Have biweekly team meetings in which the manager would reinforce in didactical activities security guidelines and protocols. |
| --- |

### 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. Conditional Access  This would be an administrative type of control implementing a multi-factor identification with the goal of preventing the usage of personal devices to access work information.  One of the possible advantages of this implementation could be real-time tracking of login failed attempts, allowing management to address the issue, which also forces the users to use the right login requirements.   One of the possible disadvantages is that if not set properly could have quite some limitations that would slow down work activity.  Answer based on the reports from:  Access control <https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview>  Access control disadvantages and limitations  <https://practical365.com/five-most-common-conditional-access-misconfigurations/>  <https://learn.microsoft.com/en-us/defender-cloud-apps/caac-known-issues> |
| --- |

| 2. Provide Devices such as work phones and computers  This solution is not the most budget-friendly, but it provides a mixture of technical and perhaps administrative approaches targeting goals such as:  -Preventing and deterring the exposure to risks because it can follow company guidelines of security. -also by correcting the habit of employees trying to do such on their personal devices.  One of the advantages is the ability to track and monitor activities within the device and can be provided with a secure VPN to avoid MIT attacks.  One of the disadvantages of this method is that the device could be lost or stolen which could lead to data leakage and data loss. |
| --- |

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