| 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.

| Lost or stolen devices seem to be the most common. There have been reports of data breaches at organizations due to stolen devices. This is typically done by introducing malware into the organization's network. According to various studies approximately 25% of suspicious activity reports show that the victims know the suspected thief through various different avenues. |
| --- |

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 would be to use encrypted devices to mitigate lost or stolen devices. Additionally require installation of an anti-malware product on personal devices. Require the use of a VPN to access the organization's network for employees that are working off site or from home. Lastly the biggest preferred behavior would be based around increasing the awareness of each individual employee. |
| --- |

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.)

| Utilize the Information Security Culture Framework (ISCF). Through an assessment questionnaire employees will provide data around their demographics (Age group, education, background, job title, information technology use and experience), specifically around their perceptions, knowledge, beliefs, and overall knowledge and practice around InfoSec. |
| --- |

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.)

| Before setting a specific goal you would need to wait on the results of the survey. Once this has been completed and then verified reliable with valid data, the goal would then be to a 50% reduction with the end goal of being at or below 5% overall. Also any required learning specifically around information security will require an 80% grade. |
| --- |

### 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.

| CEO in order to provide information regarding the existing state of the company. Brings all required/ involved parties to the table. Provides resources for the execution of proposed plans like buying required software, new daily equipment like laptops or phones for your employees.  CIO to implement any technology based steps of the plan, such as installing software, upgrading software or Operating Systems, encrypting employees personal devices. Will also conduct surveys for the Security Culture assessment and track improvements towards goals that are implemented from the assessment results.  COO to communicate any and all policy changes to employees. Training employees through awareness courses or programs.  Chief of Staff for hiring new personnel as needed for the implementation of the new security culture. Such as new IT specialists. Also communicates the security risks to the lower managers and setting up VPN for work from home employees.  CFO to determine the financial feasibility in instituting the new company policies. For example determining if the company is able to afford any of the new equipment, software or staffing needs to fulfill the plan. |
| --- |

### 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)?

| All new employees and employees that are deemed necessary to be onsite will conduct the training(s) in person. All personnel that are currently working from home will be allotted the option to complete the training via zoom or other online learning platform. At minimum the courses will need to be completed every 6 months or every time a violation has occurred. |
| --- |

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

The live zoom session will be a welcome orientation as well as the 1st mandatory training session regarding cybersecurity policies of the company. The company’s leadership will participate in the live session including the Chief information security officer, chief information officer, Chief operations manager and if feasible the company’s CEO. This session will emphasize company’s policies in the cybersecurity culture. The topics will include:

* 1. State of the company: The designated officials will share statistics regarding the company’s employee's and the risk of cybersecurity threats. Any relevant data regarding the past incidents will also be shared.
  2. Emphasizing the company's culture that cybersecurity is "everyone's responsibility"
  3. Information regarding who to contact and report if an employee suspects a data breach, receives a suspicious email etc.
  4. Introduction to reward programs for compliance with the cybersecurity policies or reporting incidents.

In addition to the in person/live sessions, the employees will also take additional courses to create awareness on specific categories of cybersecurity insults. The courses would need to be taken on an annual basis with an update on the new security risks

* 1. Phishing scams: Emphasizing not to click unfamiliar links in external email. Emphasizing the company's administration will never ask the employee's to directly provide passwords etc.
  2. Information regarding the common types of hacking tricks such as malware, ransomware, form jacking, code injection, brute force with examples of data breaches with other companies
  3. Online training with the installation of anti-malware software on the employee's personal devices
  4. Certain employees maybe more vulnerable, especially if they need to routinely perform work related activities from home. For example, residents who need to obtain access to electronic medical records of patients from home. Such employees may be better off using company's issued devices with secure encryption at home. An alternative will be encrypting the employee's personal devices (if they are willing) for remote work.
  5. The employees will be educated regarding the 2 or 4 factor identification system to prevent identity theft. The online training will inform the employees with examples regarding the mechanisms of identity theft along with videos of how to set this up at the start of their employment
  6. The employees will be educated about the company's policies of not using external USB, how to obtain encrypted USBs for work that maybe issued by the company if needed.
  7. The training will also include information regarding the alternatives to using personal devices at work such as remote desktop connection, working on the server that is protected against a firewall rather than personal computer for any data related activity. Using encrypted USBs issued by the company rather than the external USBs.
  8. Adopting common sense measures including logging out before leaving a computer, limiting access to confidential information on a need-to-know basis. Not disclosing protected information on social media. Reporting incidents of potential data breaches i.e. lost or stolen laptop

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

| The effectiveness of the cybersecurity culture framework will be assessed by evaluating the three dimensions   1. Measuring awareness: This will include results of the quizzes, participation level in the training programs. Testing employee's knowledge by conducting surveys and comparing results for before and after training using the same survey. Another method is by assessing employee feedback 2. Measuring behavior: This can be achieved by simulating phishing attacks and measuring how many employees fell into the trap. 3. Measuring culture: Performing analysis to determine the culture of the institution by reviewing patient's feedback. Identifying recurrent topics and obtaining a sense how seriously do the employees take the cybersecurity threats. Determine whether these perceptions have changed with the implementation of new policies. I would conduct this cybersecurity culture analysis on a yearly basis. |
| --- |

### 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 1 here] |
| --- |

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

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