| 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.

| Data Theft, Malware, and legal problems are all possibilities that can happen |
| --- |

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 for malware is to have only administration have the ability to install software on company based equipment. |
| --- |

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 use regular scheduled training on the practices that's supposed to be used by company policies. |
| --- |

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 would be to have 0 malware on the network from reckless usage. The admin placement should take away from the causes. |
| --- |

### 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.

| Network Admin: This team member will be in charge of overseeing the servers and allowing access to the network via new faculty and staff.  Cybersecurity analysis: Their role is to secure the network internally as well as externally. To defend against cyber attacks on the network as well as employees that use the network.  Helpdesk support: To assist people within the company with tech based problems., As far as locked accounts, key card creation,ect.  Desktop team: To assist people within the company with tech based problems. As far as onboarding new team members, control of warranty replacements, fixing issues with computers, printers, etc.  Automation: Jobs is to write script in code for the automatic processes that help they company run on a day by day bases |
| --- |

### 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)?

| I will be running online training every three months |
| --- |

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

| A couple of topics include training of phishing scams, understanding tailgating, not allowing others to freely hold personal or company devices. |
| --- |

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

| I will have the analysis team run numbers and charts on the amount of phishing and social engineer trick that happened three months before training and stats on three months after. |
| --- |

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