| 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.

| Device Theft Malware Data Leakage |
| --- |

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.)

| Devices only stay at home Company Provides anti malware to all BYOD related items Users use VPN tunneling for accessing/depositing on premises resources |
| --- |

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.)

| Have location services enabled on all devices that utilize company data to track location Run a scan daily on BYOD devices for malware detection Packet sniffer (like wireshark) running on BYOD in background for reporting visible traffic if with company resources |
| --- |

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.)

| All employees utilizes the VPN during work hours, 95% of employees have their devices registered with the antimalware endpoint agent. |
| --- |

### 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.

| **CIO** - This person will be leading the front in communications to the CEO/ company for the implementation of these services/ policy. All reports are sent to them. **System admin**- This person will setting up back-end services and configurations for all technical aspects. This includes but is not limited to enrollment in MDM services for all BYOD tech. **Helpdesk department-** Their role is to troubleshoot any issue that comes up in terms of connectivity and software related issues the user is facing. They are the front line for issues being reported by users and escalate to the security unit.  **SOC Unit -** They will be monitoring all machines for any anomalies within the anti-malware and VPN services. Ensuring all devices are patch and report to the system admin otherwise  **All other Employees**- Their role in this is to report anything that seems out of the ordinary and participate in training. They will report anything and anything fishy to the Helpdesk if not already detected by the SOC |
| --- |

### 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)?

| Training will occur bi-weekly awareness training in a 3 month roll-out period over the course of 1 year cumulatively, in the format bite sized online video segments going over the different kinds of attacks. They will be quizzed once a month on the training they have received and all quizzes will contain the cumulative knowledge they have learned. |
| --- |

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

| Risks of phishing due to how common it is and how no one is safe. Risks of Malware for the impact it can have on a company and personal devices How to properly use work devices from home - this can be multi-segmented since this can include registering for the program, the systems requirements, behaviors online, do’s/dont’s of BYOD… etc |
| --- |

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

| To measure the effectiveness, after 3 months have passed post training, simulated attacks will be pushed to each user. Based on how they react (reporting or doing nothing) they will be contacted and told their success/failure. If they fail they will need to do more training over a longer period of time. |
| --- |

### 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?

| Geo-fencing - Technical control - preventative/ Compensating control Advantage: Device will only work in approved locations Disadvantage: Device will not work outside of approved locations - in the case of emergency or business trip the user cannot work on the device |
| --- |

| Password Encryption policy on all files related to the company - Administrative control - deterrent control type Advantage - ensures authenticity/integrity of the files Disadvantage - could require training for all users that do not know how to do so and also is a time-sink for large files when compressing |
| --- |

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