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

## Assessing Security Culture

Make a copy of this document to work on, 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.

| The risks that are involved in allowing employees to view work information on their personal devices are that the employees will not protect said data as sufficiently as they will at work, making them easier to target and exploit.  Phishing attacks are also a big problem due to employees being more carefree on their personal devices, such as clicking on links from an email they do not know and, in return, giving access to the malicious actor.  Another problem with this is having your device stolen, and all company information on your device is stolen.  Malware attacks can happen from anywhere and almost anything, such as installing an app that has malware using a random USB drive or charging your phone on a public outlet. All these methods of injecting malware to your device make it easier for your or the companies information to get stolen  Phishing attacks  Malware  Device being physically stolen  https://teampassword.com/blog/byod-policies-cybersecurity-risks |
| --- |

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.)

| Referring back to the earlier query, it is advisable that staff members use separate email accounts for professional and personal purposes in order to reduce the likelihood of phishing scams. Additionally, given the rising rate of theft in NSW, it should be advised that you never keep company information on a personal device. also training employees not to use random usbs or download any malicious software on their device |
| --- |

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.)

| To measure phishing attacks, I will send out bait emails asking employees to fill out this survey for a prize, then see who has submitted the survey and give them additional training to not fall for these phishing attacks.  For tracking malware attacks, I will place usbs around the office The USB will say New Year's party on it as soon as the employee plugs in the USB device. I will than be sent a notification that the employee was tricked in using the usb  I think companies should hold training for employees to know what is safe and what is not, making these attacks less frequent |
| --- |

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.)

| I think the goal for the company to achieve is 0% but that is impossible and the company should aim towards less than 15% for all attacks |
| --- |

### 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. CISO: As head of security and person in charge of the company's security through implementation and enforcement of security policies and procedures, the CISO has to be present at the training. 2. CEO: The CEO is responsible for supervising all aspects and approving training and additional training when necessary, all while making critical decisions for the company 3. CFO: As the head of finance, the CFO oversees financial planning and provides information on the price of initial and ongoing training. 4. Security manager: a security manager ensures there is little to no data or assets stolen from the company They construct security measures in order to protect the company. They would be overseeing all activity in the training. 5. Guard: They watch over the front of the building to ensure that no one is tailgating and to verify the identity of the staff. |
| --- |

### 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)?

| 2 times a year and a combination of both |
| --- |

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

| 1. The most common and simple type of cyberattack is phishing. phishing attacks and emails will be included in training because there are more than a trillion of them sent out annually, and 323,972 internet users fell for them in 2021. 2. Passwords are the most important thing, and the first thing you should do is create a strong password. Avoid using the same password on several websites, and never enable autofill. To reduce the likelihood of a breach, you should take extra precautions and change it every three months. 3. Connecting to unsecured wifi can result in man-in-the-middle attacks and hackers injecting malware. With more people using personal devices for work, doing your work in a cafe with unsecured wifi can expose your companies data to hackers 4. DDOS attacks prevent users from accessing certain data. There are around 30 DDOS attacks daily, and being able to recognise and defend against DDOSing is important and crucial to running an operatible company. 5. Encryption is an important aspect i think we should include in training because, if there is a breach, having data and emails encrypted also puts an extra line of defence in place. |
| --- |

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

| I will measure it by doing quizzes and surveys, sending out fake phishing attacks, and holding test before and after the training to see what has improved and what has not |
| --- |

### 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.

<https://www.investopedia.com/terms/c/ceo.asp#:~:text=The%20CEO%20is%20responsible%20for,public%20face%20of%20the%20organization>.

<https://www.cisco.com/c/en/us/products/security/what-is-ciso.html#:~:text=A%20CISO%2C%20or%20chief%20information,policies%20to%20protect%20critical%20data>.

<https://www.netsuite.com.au/portal/au/resource/articles/accounting/chief-financial-officer-cfo.shtml#:~:text=The%20chief%20financial%20officer%20>(CFOs,weaknesses%20and%20proposing%20strategic%20directions.

<https://aag-it.com/the-latest-phishing-statistics/>

<https://securitybrief.com.au/story/ddos-attacks-not-only-more-frequent-but-more-powerful-report#:~:text=Attack%20frequency%3A%20The%20frequency%20of,at%20the%20end%20of%202021>.