| 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.

| The potential security risks of allowing employees to access work information on their personal devices include accidentally downloading malware to a personal device by downloading a compromised personal application, allowing access to the personal device via unsecured public networks, and running the risk of the personal device being lost or stolen that would allow for confidential data to become compromised. In these scenarios, a hacker could easily gain access to extremely sensitive corporate data and can use this information for personal gain or to exploit a company’s integrity. |
| --- |

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 separate personal devices with work-related devices for the benefit of the person’s standing in the company and for the company’s sensitive information to be protected. If this cannot be done, then the preferred employee behavior for downloading personal applications would be to strictly download personal applications to personal devices only and to have the company’s cyber security team vet the applications on their personal device to flag any at-risk applications. For connecting to public networks, the preferred employee behavior would be to only connect to secured networks with at least a password for logging in and not to any kind of public wifi network open to the public. The preferred employee behavior for losing a personal device would be downloading an application that could track the personal device’s whereabouts as well as having a way to shut down the personal device remotely so that whoever locates the device cannot access what is inside the 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.)

| The methods I would use to measure how often employees are currently not behaving according to the preferred behavior would be to conduct a risk assessment on the employees’ personal device if they in fact used it for work. I feel like that is a fair request since the device being used can affect the company. I also would educate the employees on the importance of having a strong security culture within the business so that they are aware of the dangers of cyber attacks and the harm that they can cause for both parties. There would be training exercises of things to look out for and what to do if they feel that their device has been compromised. A proactive approach can really benefit a business ahead of time instead of a reactive situation in which it may be too late to fix. If we have strong participation in this scenario, the company has a real chance of being protected properly. |
| --- |

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.)

| Understanding that personal devices are being used for work-related activities, I feel like it is impossible for any company to have 0% in the area of cyber attacks. Accidents happen and no one is perfect. Even if we do everything correctly, nothing is 100% perfect. However, I believe that having less than 7% of employees become cyber victims would be fair for the initial rollout of the training. This would be for employees that completed the training in Q1 and I would monitor the progress of those specific employees for the remaining three quarters to complete a full year. The goal that I would like the organization to reach would target less than 3% by the time that they completed the training the following year and would like to see that number remain or improve for the following year and so on. Of course, there are going to be new employees and new dangers in the cyber world that could alter these numbers, but that would be my goal as one who would be handling the security of the company’s data. |
| --- |

### 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. CEO - The leader of the company must be involved because they are responsible for knowing all of the inner workings of the company. They must be in the loop regarding risks, plans of action against those risks, and to oversee employee behavior to mitigate the risks. 2. Security Culture Framework Team - This team is responsible for rolling out the cyber security framework and to develop the training for employees to be aware of cyber dangers. This is the go-to team for any concerns regarding the security of employee devices as well as providing guidance for the employees who may have been compromised. This team is the point of contact for all cyber related questions. 3. Human Resource Team - HR would have to be involved to determine when the best time for cyber security training would take place. We need to have every employee participate in the training and with work that needs to be done, there could be a challenge regarding work schedules. Working with HR to make the training mandatory would ensure that the training would be completed in a timely manner. 4. Communications Team - This team would be responsible for relaying the information of the training to the employees and to make sure that every employee understands the training to the fullest extent. They also could assist the Security Culture Framework Team in collecting data from the training exercises to determine the results of where the company currently stands regarding security. 5. Legal Team - Since we are going to implement rules and regulations for the company, the company’s legal team needs to determine what we can and cannot do in accordance with the rights of our employees. The company needs to make sure that the guidelines we put in place are not in any sort of personal violation, since we are talking about employees using their own personal devices for work. |
| --- |

### 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 would run training in-person for 25% of employees during Q1 with the goal of every employee having completed the training at the end of Q4. The following year, I would collect all of the data on the progress of these implementations and see where we need to improve or which employees have had the most issues with their personal devices. If we do not meet our goals, we would have to revisit the training procedures and make adjustments accordingly to improve the numbers. If an employee is a repeat offender, there will be an employee review to determine if that employee has become too much of a liability with carelessness or the possibility of the employee not taking the training seriously. I would run in-person training because there is always a higher possibility of people making excuses for an online format. In-person would ensure that everyone is on the same page at the appropriate stages of the training. |
| --- |

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

| The topics that I would cover in my cyber security training include Risk Management because it carries a lot of weight in a business environment. Customers and clients alike want to do business with a company that is safe and they can trust. Providing guidelines for risk management will allow our patrons to trust that their information is protected and feel more comfortable doing business with the company that takes their data security seriously. Another important topic is Disaster Recovery and what steps we need to take in order to get the business back up and running in the event of a security breach. It is inevitable that threat actors will find a way into a network, so having a plan for what to do when that happens is very important. The Business Continuity Plan is key to review because it is the framework in which we make sure that the business will thrive and will be protected. We can ensure that we are taking the appropriate steps in mitigating risks for the company by having a plan for our security expectations. Security Concerns versus Business Concerns are also important to go over, considering that even though we must make security a priority, there will still be business opportunities/situations that arise and need attention. The goal here is to make sure that we conduct business in a safe environment and not to fall victim to an adversary that is trying to take advantage of the business, especially when we conduct business online. I would also include the company’s policies in regards to how an employee should use their devices, whether for personal use or for work, and how using those devices the wrong way can lead to dangerous consequences for the company and the individual. The company’s compliance with these policies will also be reviewed to make sure there will not be any surprises if the worst should occur. Every employee must agree to the terms of the consequences if the employee does not comply with these policies. Also, I would incorporate how to mitigate risks by showing the employees a number of ways that we can make sure cyber criminals are kept at bay. Learning how to mitigate risks is crucial to keeping private information secure by eliminating a number of ways that a hacker can gain access to confidential data. Reinforcing the security of one’s device can help block hackers and discourage their attempts at breaching our networks. Finally, after all of these topics have been covered, I would finish the training with an explanation of the qualitative and quantitative impacts that cyber risks can have on a business and what the differences are. Even though business is mostly quantitative when talking about numbers and figures, the thing that gets overlooked is the impact that cannot be measured in numbers. The reputation of the business and its vulnerabilities affects everyone in the company. Even though the goal is to make as much money as possible, how you do it and the measures you are taking to make money are vital to how a business should operate. Sometimes, a problem can go away with throwing money at it, but other times it is better to do the right thing and invest in security. In short, I believe most clients would rather do business with a company that is more secure/safe than a company that just has the most money. Balancing these two aspects evenly can lead to an extremely successful business. |
| --- |

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

| I would measure the training by doing a lot of pentesting and phishing. I personally feel that is the best way of determining who is taking the training seriously and also acts as a real-life scenario exercise for the employee to apply the tools and knowledge that they have learned through real-life situations that happen every day. I would collect the data from those who passed the tests and those who did not and try to determine which employees we need to look closer at and who we do not need to worry about. Phishing is one of the most common strategies used by hackers and if we can prepare employees by utilizing this method specifically, then they are more likely to avoid the attack and keep the company safe. |
| --- |

### 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.