| 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.

| When utilizing a bring-your-own-device (BYOD) approach to a work environment, a company opens itself up to quite a few risks. Should a user’s device get stolen, any information that might be stored on that device could be compromised. Additionally, emails on that device would be open to whoever stole the device, allowing them to phish for information from an internal email address.  Another thing to consider would be if the user’s device has malware on it. By plugging into the network (or a USB into their computer which then goes onto the network), they could be infecting every computer unintentionally, causing not only compromised accounts, but potentially financial loss for the company, and for any companies they work with/for.  Another thing to look at is the opposite side of things, where an employee takes sensitive information out of the office on their personal device (which isn’t monitored because it is not company property), and if they are disgruntled/fired/approached by someone, they could then sell that information to whomever. Not only would this be a serious breach of the company they work(ed) for, but it could be financial/reputational ruin for that company as well. |
| --- |

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 behavior would be to not allow a BYOD policy. However, if it is an absolute must, then enforcing a strict policy of security enforcements would need to be put into place. Any device attached to the network would have to have an up to date AV on that device. Additionally, those devices would have to be approved by the IT department for use. If a thumb-drive is needed, then that drive must be encrypted (preferably something like an Apricorn encrypted flash drive), and will be provided by the IT department. All devices will have a MFA account attached to them, in the case that something is stolen, and a password is compromised, then there is still another step which must be taken to get into the account. VPN’s would also be utilized along with the MFA account for any access to company systems outside of the company network. |
| --- |

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.)

| With the above factors put into place, it should be easy to monitor anything that might be happening on the company network which might compromise the company/systems.   For those systems which are not as easy to monitor (such as clicking on email links/attachments), a regular phishing campaign should be implemented. By utilizing this, you can see who your problem children are and focus training around what they are doing and seeing.  From there, making sure that everyone within the company goes through training regularly (at least annually, more so for those who fail the phishing campaign), it should reduce the instances of someone clicking on a link/attachment that could lead to a compromised account.   Also setting a strict 3-strike policy might help. 1st time, more training. 2nd time, loss of systems/privileges. 3rd time, release from company. |
| --- |

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.)

| Depending on the original metric which you are going from, a 5% reduction would be good, insofar as the issue of phishing emails. The goal should be to get to as close to 0 as you can, but that is most times a pipe-dream.  With the other issues of having something stolen or an account compromised (other than through a phishing event), that goal should always be 0 incidents.   Should something get stolen, then the employee should let their manager/IT know immediately so that those devices/accounts can be locked down, preventing access from someone who isn’t the rightful employee (or a current employee in the case of a termination). |
| --- |

### 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.

| First and foremost, the IT department must be involved (this includes the IT and cyber security). They will be running the day-to-day of the systems for the company, and either verifying systems to be allowed onto the network, handing out encrypted devices to use should information need to leave the company network, and monitoring all activities pertaining to the security of the information and credentials of the company’s network.  HR would also need to be involved, as they need to understand the consequences and be ready to enforce them should an employee require the 3-strike rule.  Legal would need to be involved, because if there is a compromised account and information is leaked/stolen, they will need to be able to not only protect the company’s best interest, but also be ready to provide written statements to subcontractors/clients/public of the breach, and what it might mean for them and the steps that have been/are being taken to mitigate the issues.  Finally, the CSuite (CEO, CFO, CIO, CISO, etc.) needs to be involved. It is on their shoulders if something happens which causes a problem for the company. Any loss of time/money/information will be on the employees shoulders, but it is the CSuite who will be in the public eye for the breach. They need to understand the potential problems that might arise, the steps that will be taken to mitigate the issue, and what the breach might mean for the company so that they will be prepared to address the board/public. |
| --- |

### 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)?

| As mentioned above, at least an annual training needs to take place. To me, this should be in-person, because it then requires employees to be present and accountable. Additional training beyond that annual training can be done online. |
| --- |

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

| In-person training should cover the gambit.   It should talk about the risks of bringing in your own device and using it on the company’s network. It should enforce the idea that if you do bring in your device, it must meet the proper standards for it to connect to the network. Your personal device must be approved by IT and if a USB flash drive is needed, one will be provided by the IT department for your daily use.   The in-person training should talk about the risks associated with phishing emails, what to look for with them, and what clicking on a link/attachment might do. It should go through the steps that an employee should take if they receive an email which they think is suspicious (don’t click on any links, check the email address and not just the name, call the person who it says sent it and ask them if they did send it, forward to the IT/security department for confirmation that the email is good, etc.). It should also highlight the 3-strike policy, and make sure that everyone understands it.  In the same breath, the additional training (if needed) for phishing would go over the same things.  The in-person training should also talk about the risk of plugging in a USB drive into a computer if a drive was found on the ground, or lying around and someone doesn’t know where it came from or whose it is. These kinds of devices should be given to the IT/security department for inspection and if safe, they can give it back to the owner and talk with them about the importance of not leaving these kinds of devices lying around. |
| --- |

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

| Measuring the effectiveness of the training could be done by giving random tests after the training. A test a week/month/6-months after training to see how much someone retained.   Also by monitoring metrics, you should be able to see how effective the training was. Are there any accounts which you’ve had to lock down because something was lost/stolen? How many people are caught in a phishing campaign? |
| --- |

### 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?

| The first solution I would offer goes back to now allowing a BYOD policy at all. This is an administrative control, because it would be a policy that is in place within the company. This control would potentially prevent an employee from bringing in an outside threat on their own device which they may or may not know is there. It would allow for the company to have a stricter control over their network, but for the employee, it could be a bit of a headache, especially if they do a lot of travel for the company and use a USB to store their information on. That could be easily mitigated by the IT department providing the devices which they would need to do their job, but that would cost the company more, depending on how many additional devices would have to be purchased for those employees. |
| --- |

| The second additional solution I would offer revolves around phishing emails. If the company’s large enough, and has the resources to allow it, I would say to have all emails go through an internal email server first for review/scanning prior to being delivered to the end user. This doesn’t mean that someone needs to be sitting there reading all the emails, but there are systems which can check emails to see that they come from a legitimate sender, and do not contain anything which might compromise the company or its network. This would be a technical control that would detect anything that isn’t right, and hopefully prevent it from going to the end user where they might do something which could compromise the company/network. The advantage, of course, is that it could catch something prior to it happening, but at the same time, systems can be bypassed, and that email could still get through to the end user. |
| --- |

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