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.

[BYOD in a work environment poses several risks, the main risk I found is data theft. Allowing untrained and unassuming employees to use their devices for both work and personal opens the door for a lot of potential vulnerabilities regarding data. If an employee is hacked, it could potentially lead to company information being leaked or getting into the wrong hands. Said hacking is now much more likely because an employee, probably not too concerned about company data, has the ability to make mistakes, fall for phishing tactics, etc. Data theft can be achieved in many ways: phishing, ransomware and losing your device seemed to be the most likely to me. Employees, if untrained, can more easily fall victim to phishing attacks if they are not using a more secure company device, and are more likely to be exposed in general to these attacks via personal emails, social media accounts and whatever personal browsing they do. An employee could be attacked using ransomware, if they have an unsafe connection, no protection on their device etc, which could lead to the leaking of company data, or entry into company accounts where further damage can be inflicted. Finally, something as simple as losing your phone, or having it stolen, could also become quite a tragic security breach if an employee has work info/accounts on their personal device.]

2. 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.)

[Personally, I’m not finding many reasons why letting employees use their personal devices would outweigh the risk, but proper training could prevent a lot of the above issues. Auto log outs for all company accounts would help if an employee's device was stolen or lost, provided they aren't taking screenshots, or writing anything down outside of the accounts. Educating employees on VPN’s and unsafe networks could also mitigate some risks, though the likelihood every employee uses a VPN all the time is unlikely. Ideally, all employees are well trained in phishing attacks, vpn usage and there are some failsafes out of the employees control (2 factor authentication, captchas, auto log outs, etc).]

3. 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.)

[People would probably just lie on a survey, even if you made it anonymous. I would probably start with big threats (firing or suing) if company data did get leaked due to negligence, if I was an employee that's the last thing I would want over not turning on a VPN. As for monitoring, maybe someone goes through all employees' email logs once a month to check on everybody, or phishing “drills” could be implemented every so often, where a fake phishing email is sent to everyone to see how many people engage with it.]

4. 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.)

[Ideally zero, it only takes one time for something bad to happen. But maybe with firewall or security requirements on all devices, less than 2%.]

Step 2: Involve the Right People

5. 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.

[Security department, firstly. They will be necessary in monitoring employees and mitigating risks. The security department would be the ones creating and sending the phishing emails, also working with HR to put together training for the employees. They would also be in charge of deciding what security protections should be required on employees devices, and going through logs.

Finance should be more regulated, they are dealing with more sensitive information than other departments, so they need more training. They would need to be more involved than other departments, going through more in depth training and possibly testing of some kind, as well as having more security on their devices. The rules and practices they would have to follow would be more than regular employees, so they also need to be trained on why that is.

HR to do quarterly seminars on security stuff for all employees. HR will be important, not only to help educate and organize training for employees, but also to determine what to do when someone breaks the rules. As well as handling situations that may include sensitive information.

All employees across the board should be involved in training, drills, protective measures and knowledgeable of the possible risks relating to using personal devices for work. I mention this because at the end of the day, it only takes one employee to do a lot of damage. Even a low level employee is a risk if uneducated and unprotected. Their participation in these security measures is one of the most important mitigations.

CISO should always be well informed of the risks BYOD causes. They are in charge of delegation of funds and resources to the different departments, so they will also need to stay in close contact with heads of all departments. The CISO’s devices should have the most possible security precautions.]

Step 3: Training Plan

6. How frequently will you run training? What format will it take (e.g., in-person, online, a combination of both)?

[Quarterly in person training seminars with well trained/informed instructors, the drills I mentioned above could be more frequent to see who just isn’t getting it. The training should be done in person, in a lecture-like environment, where everyone brings their devices so they can install necessary software, and participate in the activities. Online assistants after class to help with questions would be helpful, but I dont think online training would be as effective as in person training.]

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

[Phishing and social engineering, namely, the biggest risk is the employee, so educating them on that is the most important I think. Giving phishing examples, going through common scenarios and doing a hands-on activity where the employees get to show how they would react to a phishing email. Discussing what the risks for the company are, how important data security is, and even showing them how to protect themselves and their data would encourage engagement. Rather than just making it all about the company. Covering malware, ransomware, SQL injections and DDoS attacks is important too, making sure people know and understand the risks to it doesn't seem like meaningless training. Demonstrating these attacks, though maybe impractical, could showcase how easy it is to fall for them, and execute them with just a little bit of information. Separate training for departments dealing with more sensitive information will be necessary as well, everyone should get some basic training since they are carrying company data in their pocket, but certain departments or individuals will require more in depth training.]

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

[Pseudo phishing attacks, or other forms of social engineering would be the most accurate way, I think. Asking the employees might not yield truthful results. Surveys could be good too though, to compare results between the two.]

Bonus: Other Solutions

9. List at least two other potential solutions. For each one, indicate the following:
    a. What type of control is it? Administrative, technical, or physical?
    b. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

c. What is one advantage of each solution?
d. What is one disadvantage of each solution?

[Log checking, or checking email traffic. This would be a technical control, with a detective goal. Since devices are personal, there could be privacy issues, this also probably would be a good way to check personal emails, or to make sure people aren't doing sketchy stuff on their own accounts. It seems like a surefire way to check in on people and make sure they are adhering to company practices on company related accounts.]

[From an N-able article, I found a product called RMM, which protects employee devices with their software, and allows you to remotely lock phones, wipe devices and reset passwords all remotely. This, again, could pose privacy issues for the employee. Maybe someone doesnt want that kind of thing on their device from the company, but it seems like it would be a really good option. It takes some of the responsibility of updating, downloading etc out of the employees hands. And in cases of emergency, it lets administrators handle situations more easily.]