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.

There are many potential security risks when employees are allowed to access work information on their personal devices. Some of these include:

Loss and theft of the devices - apart from personal information, company information would potentially be at risk of falling into the wrong hands.
Malware and viruses - due to the devices having a dual use (personal and work), the risk is higher that these devices can become infected with malware and viruses through the personal use aspect. Company also has less control in restricting or blocking access to non-work related topics, in contrast to if the devices were restricted to work only use.
Data breaches - due to not being part of the company’s IT infrastructure, personal devices do not afford the same protections for the data on it. This increases the threat of data breaches, as the devices have a higher likelihood of connecting to unsecured public wifi and hotspot networks, as well as to the physical loss and theft of said devices.

Phishing attacks are more likely to take place. Even if the company has some security programs on the personal device, it may be inadequate to cover personal apps and other personal spaces that the user is visiting, such as internet forums. Here, a link can be clicked that could infect the device with malware and/or viruses.

Credential based attacks can occur as employee credentials can more easily be stolen, and threat actors can use these to make unauthorized purchases or transfer funds from company accounts, resulting in significant financial losses for the company. Furthermore, critical data can also be at risk of being stolen.

Eavesdropping attacks, such as a man-in-the-middle attack, are more likely to occur as the personal device will have more opportunities and freedom to travel around and connect to various public networks and hotspots. Without the appropriate protections and behaviour, it is possible for a threat agent to position themselves in a conversation between a user and an application, where they can possibly eavesdrop and intercept critical data, conversations, etc.

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.)

One behaviour preferable for employees would be for them to be extra careful on clicking any unknown links, whether it be in an email or a website, as well as not visiting any “sketchy” websites on their dual use device. This way, they have a better chance of not falling for phishing scams, as well as reducing their exposure to potential malware and viruses. Furthermore, limiting downloads to only work trusted material and to the most trusted of websites/apps unrelated to work will help minimize these risks.

Another behavior is to simply be more careful and aware of their surroundings in order to avoid the physical loss/theft of these devices. Furthermore, implementing a security feature that locks the device, such as a password, facial recognition, etc (if possible, more than one feature) should be mandatory as it provides an extra layer of defense should the device get lost/stolen.

A third behaviour would be to have employees create strong passwords that contain various different types of characters (i.e. numbers, different capitalization, special characters, minimum length), and to have them change it on a predetermined basis (i.e. every month, quarter, etc).

Finally, in the event where an employee is required to use their device on a public wifi network or hotspot, then they should use a VPN, firewall, and antivirus software in order to filter the traffic that can enter the device, and decrease the risk of attacks such as man-in-the-middle attacks.

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.)

A mandatory survey would be a first step to measure how often employees are following the guidelines for their dual use devices. It is probably the least invasive method, however, it will undoubtedly be less accurate than actual verification (i.e. physically reviewing device logs with respects to locations visited, browsing history, connection history, etc). Some questions to ask on the survey would be: 1) how often do you take the dual use device out with you during non-working hours? Does it go everywhere you go? 2) What sort of vpn, firewalls, and anti-virus software is installed on the device? Is it routinely kept up-to-date? 3) What sort of security features are enabled on the device to control who can use it?

In order to measure the click-through rate, I would get someone from IT to send out fake phishing emails on a routine basis, and calculate how many employees are clicking on the links and thus not following the preferred behaviour guidelines.

A third method would be to monitor the log-ins to see how many employees are logging in from public networks (as opposed to the preferred private networks), and how often they are doing this.

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.)

I don’t think that employees should be limited to where they want to work (outside of the office), for example at a library, coffeeshop, etc. From the point of view of the organization, it is therefore crucial that they follow the preferred behaviour guidelines at all times, and that they are observable and enforceable by management.

I believe the goal for ensuring that the dual use device has appropriate vpn, firewall, and anti-virus software installed could be enforced to 100% compliance rate. A technical control should be imposed where an employee’s login will only work if the login portal is able to detect the use of the above 3 tools, and ideally that they are up-to-date.

With regards to phishing attacks and malware/viruses due to clicking on unknown links, I think it is reasonable to get this to under 3% of employees. I don’t think that 0% is possible, as accidents are bound to occur at one time or another.

Creating strong passwords should be set at 100%, as this can be a technical control that will force employees to reset their passwords at predetermined intervals.

Ensuring the devices have security features to limit access (such as pin code, facial recognition, pattern code, etc) should be at least 95% or higher compliance.

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.

Human resources department - in the hiring process, they need to make sure that candidates are of good integrity and ethics. Ensuring they provide criminal background checks is one way. Following up on references to ensure that the potential candidate is not of a nefarious, or incompetent/careless nature is also a good practice. With regards to training and orientations, HR will help to coordinate the dates and times with management to find the best way to ensure full attendance for these sessions.

Finance Department - responsible for securing the funding that is needed to ensure these programs and procedures can go ahead and work effectively. Doing a quantitative analysis will help answer questions such as “Do we have the money to implement all these systems? Is our bottom line shrinking/growing, in order to determine how much money might be available going forward to develop and maintain such systems/controls?” Ultimately, they will be directed by the CEO on what controls the organization intends to deploy, while advising the CEO on the costs of said deployments.

IT Department - they will be responsible for setting up all the technical controls that will help keep the organization’s data and systems as safe as possible while allowing employees to use their personal devices for work. They will report to the Chief Information Officer, who will ensure that the I.T. systems being developed are compatible with the organization’s functions and goals, as laid out by the CEO. Implementing an efficient log system that can easily be accessed and observed by the managers/supervisors will be crucial in supervising the staff’s commitment to security.

Chief Information Security Officer - will need to determine the appropriate level of risk to the organization’s data. Will require working closely with the Chief Information Officer on how to keep the appropriate data accessible to the employees while developing the technical controls to reduce the vulnerabilities due to the work being done on personal devices. Furthermore, will determine the appropriate goals for achieving the level of security that is required. This could include setting the rate goal as a percentage of employees that fall victim to phishing scams.

Supervisors/Managers - they need to ensure that employees complete all the training requirements. Will be the liaison with the IT department and the various Officers (COO, CIO, and CISO) on the continued monitoring of standards and logs, and provide guidance/discipline for when the standards and preferred behaviours are not being followed by employees.

Chief Operating Officer (COO) - once the systems and controls are developed and implemented, the COO should take over as the liaison between all the other officers, management and supervisors with the CEO. The primary goal of the COO is to ensure that everything is running smoothly on a day-to-day basis, followed by weekly or bi-weekly meetings with the CEO to evaluate how the systems are working, and to make changes and updates where appropriate. Other officers will frequently be involved in such meetings, as their technical skills and oversight of departments will be required to complete thorough analyses.

CEO - The CEO needs to decide how much of the security precautions need to be implemented without sacrificing too much productivity and efficiency of the organization’s primary goal of making a profit. The CEO will need to take into account advice from his Chief Information and Chief Information Security Officers to determine the appropriate level of controls in order to protect the valuable information of the organization while still remaining competitive in the market. In other terms, the CEO and other Officers of the organization will be engaging in both qualitative and quantitative analyses.

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)?

A combination of both online and in-person training would be optimal. Online training should be done at least quarterly, although there will be special circumstances where employees that are seen as not following the guidelines and rules will be subjected to more training (this would likely be a part of the disciplinary process, and should be promptly done).

In-person training, in the form of meetings and workshops should ideally be done semi-annually, with assessments done to ensure that the employees understand what is required of them. Apart from the managers and supervisors, the CIO and CISO should take part in these (ideally take the primary role) and really emphasize how important it is that the employees internalize the guidelines and rules to ensure data and network safety. Also, they should go over and examine the shortcomings and incidents that may have popped up in the previous two quarters, with the goal of minimizing or even eliminating them altogether going forward.

All new employees will require this sort of training in their orientation, and will need to pass an online test after in order to gauge their competency.

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

First, we will go over the various types of threats and vulnerabilities associated with the use of personal devices for work. The employees need to be aware of what can happen if they do not follow the guidelines and rules, and how it can impact the organization negatively.

Once they are aware of these threats and vulnerabilities, we will move on to their responsibilities to ensure these are minimized. This will centre around the various security controls, which are administrative, technical, and physical. A layered defense is the best practice to keep the data and employees of the organization safe.

For administrative controls, the employees will be educated on the importance of these training initiatives and how they are there to help them follow the guidelines and rules as laid out by management. More specifically, something along the lines of a download policy will inform the employees on the types of links they should not be clicking on, under any circumstances.

Moving on, the technical control aspect will encompass the bulk of the training, as there will be several technical controls implemented to ensure the data of the organization is well protected. Some of these will include how to use various programs like the firewalls and VPNs, anti-virus software, and log-in portals, which the IT department will help develop and/or install to the devices. A heavy emphasis on the dangers of using public wifi networks and hot spots will be taught. Another one would be the frequency of changing one’s password, as well as its complexity in terms of various characters used, or by requiring them to use a secure shell. The importance of these procedural controls will help the employees get into the habit of treating security as an ongoing, maintenance-like task as opposed to a one time, set-it-and-forget-it type of behaviour.

Physical controls will largely teach the employees on how to physically secure their devices. This will touch upon the importance of not leaving a device unattended in public settings (i.e. coffee shops, libraries, even at the workplace). Loss and stolen devices are a major risk to the integrity and confidentiality of an organization’s data. However, loss and theft are almost guaranteed to occur at some point, so training the employees on ways to secure their devices so that they cannot be accessed by anyone else will also be covered. Locking ones devices with pin codes, facial/fingerprint recognition, and multi-factor authentication (also a technical control) will be emphasized, and implementing a zero-tolerance policy to this end should help motivate the employees to make these physical controls a habit of their everyday lives, not just with regards to the organization.

Overall, the goal of the training will be to develop a healthy security culture within the organization. Motivating the employees to value security and how to avoid insecure behaviour through the use of administrative, technical, and physical controls are tantamount to achieving this goal.

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

Logs will be required to help the IT department determine how often and which employees are engaging in unsafe behavior, such as connecting to the company portal from unsecured networks and public IP addresses. If there is a higher percentage than what the company’s goal is (let’s say about 3% of the time), then implementing more training, and potentially discipline, for the employees involved might be a solution.

Getting the employees to periodically do a “pop quiz” every month or so on the topics and best practices outlined in their training will give management a better idea of how much the employees understand and have implemented.

Pentesters will be a useful tool to see how many employees are opening emails and clicking on dubious links/downloads that they should not be. This will help management determine if supplemental security awareness training is required, and for whom. Furthermore, if the clickthrough rate exceeds that which the company sets as its goal, or alternatively starts increasing over time, then adjustments to the training programs can and should be implemented to make it more effective.

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?

```
[Enter Solution 1 here]
```

```
[Enter Solution 2 here]
```