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.

Employees using their personal devices for work related tasks can result in a multitude of potential risks, such as data breaches, employee login credentials being exploited, lost or stolen devices and employee work and personal information being mixed, resulting in possible confusion and difficulties separating work and personal affairs.Three potential attacks which could be carried out are WiFi spoofing, man-in-the-middle attacks and malware attacks.

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.)

Given the risks involved employees, there are three primary behaviours which employees should comply with. These include using VPN services, 2FA implementation and the inclusion of remote-reset capabilities on employee devices. Employees should use VPN services when outside of the work environment to reduce cyber threats when accessing public networks and domains. Furthermore employees should use 2FA when using company communication platforms to tighten security and strengthen overall security measures to reduce the risk of company data being intercepted and exploited for malicious intent. Promoting employees to integrate remote factory-reset capabilities as well keeps information secure and reduces the risk of data/information breaches in the event of a lost or stolen device.

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.)

Implement VPN usage logs and access logs for employee devices which can be viewed by administrators to observe and identify potential employees who are not using VPN services where necessary. As for 2FA, create policies which employees must acknowledge and then set up on their devices in order to access company communication platforms when outside of work. The same kinds of policies go for employing the integration of remote factory-reset capabilities too, as this notifies the company of who within the business is yet to implement these new changes.

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.)

Have a minimum of 75% of employees using VPN services when outside of work. 2FA configured on all employee devices in 30 days from initial training/policy implementation. Over 50% of employee devices are configured with remote factory reset capabilities from within 30 days of initial training.

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.

IT Department:
Are responsible for the implementation of VPN, 2FA and remote factory reset capabilities on employee devices. They will also be responsible for providing

additional technical support and information for employees encountering installation issues during the training process. Both the IT and HR departments will work collaboratively to facilitate training and installations.

HR Department:
Their main responsibilities will involve curating employee training sessions/meetings for implementing new device policies. The HR department will develop weekly surveys to send to employees so device usage can be monitored and reviewed and will also have a role in allocating and scheduling employee training. Will also explore the legal matters relating to remote factory reset options for employee personal devices.

Research and Development Department:
Will be responsible for the development of VPN and 2FA software for employees to implement on their devices. They can also research into the prospect of migrating to new social platforms for work communications if Slack doesn't allow 2FA.Will involve further collaboration with the IT department to reference administrative information which will aid in development. Online training programs for employee orientations before face-to-face training is scheduled will be curated by this department too.

CEO:
The CEO will be responsible for final implementation of these policies and procedures and will be the primary figure who will oversee policy transitions and policy implementation. Roles include organising regular meetings with other respectful departments to review the policy developments and to make sure that policy targets are being achieved.

Finance Department:
This department will be responsible for calculating the total costs of these policies, which includes the execution and maintenance of VPN services, 2FA and remote reset procedures. They will liaison with the CEO as well as with the IT and Research/Dev Departments to make sure all company goals are aligned for the given budget for the project and will account for additional training costs for employees.

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)?

Employees will be required to complete a 60 minute online training course for cyber security education, which outlines ways in which they can protect themselves within the cyber landscape. Upon completion, 30 minutes of face-to-face training will be organised through the business within small groups to facilitate and manage new systems which will include setting up VPNs, 2FA and remote factory resetting on employee devices. Policies will be acknowledged and signed by employees during this period. Upon completion, employees will have a 7 day adjustment period where they can contact IT support and other resources for additional information.
After initial training, recurrent training will occur every 6 months via a 20 minute online recap course to solidify employee knowledge, understanding and compliance. Fortnightly surveys will also be sent to all employees in relation to online security and security concerns they may have.

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

Online Training:

Cyber Security Introduction - Threats and Basic Understanding

Highlighting the dangers and risks within the cybersecurity landscape. This will include highlighting possible threats such as phishing, malware and the risks of accessing public networks. The topics will identify the more common attack types and how they are executed to target individuals as this will educate employees on ways to identify and report these threats so they don’t fall prey to these kinds of attacks. Training will also highlight the importance of using antivirus and firewall software on devices, as these may both be the first line of defence when defending against cyber attacks. The training will also provide real world examples of cyber threats and attacks so employees understand how these malicious incidents are executed and orchestrated by threat actors, therefore allowing them to be more prepared in case they ever encounter similar circumstances

How to Protect Yourself Online:

This will be shown through how to use VPNs and 2FA and will also outline the importance of using secure sites such as HTTPS and show ways to stay cyber safe when on public networks. Employees will be given online resources for further information, as well as relevant contact information for IT departments when they are setting up their devices in future face-to-face training sessions. These topics will be covered to give employees foundational knowledge on cyber security topics and also means less time is necessary during work hours for extended face-to-face training sessions.

Quiz:

Upon completion of online theory, employees will undergo a 20 question quiz to demonstrate their understanding of the topics outlined. This is also sent to the HR department as they can review results before face-to-face training to provide additional support to employees if necessary. This also gives them an opportunity to identify various topics and areas which should be highlighted again during the second series of training sessions if required.

Face-To-Face Training:

The primary focus for face-to-face training will be on hardware setup for both VPN software, 2FA for devices and remote factory resetting software. These topics aim to familiarise employees with software and their corresponding processes and give them the opportunity to explore and ask questions to gain proficiency before stepping out into public domains where they will be required. This will also involve cross checking employee device details, which include the type of phone (brand, model etc) to give the IT department a more refined idea of the types of devices in use and allows them to configure remote reset controls for each user if necessary. There will still be a theory based aspect of the training, where instructors will cover the same topics mentioned in the online training, however they will only cover areas where employees require further assistance. This gives employees the opportunity to ask questions and refresh their knowledge with an instructor in-class and iron out any risks and concerns they may have. Upon training completion, policy acknowledgement documents and privacy policies will be signed by employees so they understand their responsibilities and roles once these new procedures have been rolled out.

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

Fortnightly surveys will be conducted, these will be sent out to employees company emails to be completed.

- 1 week after face-to-face training, surveys will be sent out to monitor policy effectiveness and VPN usage requests will also be reviewed.
- IT support will be monitored and reviewed to observe if employees have difficulty with latest policies after their training
- Review VPN logs on a weekly basis to identify and observe trends or areas of possible exploitation
- Require employees to submit traffic logs on their devices and application usages results. This would allow you to cross check public network times with what is currently running during that period.

- Employee devices will be reviewed and emails sent out 1 week after training to make sure that all new safety procedures are in place.

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?

Integration of employee work phones to homogenise business devices.

a. This is both physical and technical because:
    i. It streamlines and makes all employee's physical devices the same, to have a consistent level on security across all devices
    ii. All hardware, and software especially, is the same, aiding the IT department and making patching and online security easier to manage and tackle
b. The goal of this control is to have preventive measures in place
c. The advantage of this solution means that all employee work devices are the same, meaning it is easier to integrate these new security policies across one kind of system rather than multiple OS and devices. This also means less training is required for both the Research/Development and IT departments.
d. The disadvantage is this will cost more money to purchase new devices for the company and also, if these devices are exploited and attacked, that may leave the company more vulnerable as all devices can be targeted and exploited in the same way.

Implement Intrusion Detection and Prevention Systems through Mobile Device Management Policies

a. This is administrative and technical
b. This is both a detective and corrective control

c. The advantage of this means that all employee devices are constantly monitored and device usage can be reviewed and broken down to identify potential risks and threat hotspots within public networks

d. The disadvantage of this of course is the lack of employee privacy and as well the additional cost to implement IDPS across all devices. This will also impact working hours of the IT department if consistent and regular device monitoring is required.