**Week 2 Homework: Assessing Security Culture.**

**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 used in a corporate setting can be a significant risk if the devices go unchecked. Here are 3 attacks that can be carried out:

Ransomware:

Ransomware via phishing can cause data theft if an employee opens a spam email sent to their personal email. If the ransomware was downloaded onto the personal device, it could potentially get into the corporate system and hold sensitive information to a dollar value.

Malware:

Employees downloading various types of information and files on their personal devices can be a significant risk which could potentially allow malware into the device. The malware can compromise corporate security and cause issues in data breaches. E.G Keylogger could access via the malware, which can learn keystrokes, steal usernames and passwords.

Man In the Middle:

Man in the Middle attack can occur on a BOYD if the device is connected to an unsecure network. The attacker can monitor and intercept data traffic going across the unsecure network which could allow the attacker to infiltrate the company’s system.

***Refers:*** <https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember>

1. Based on the scenario, what is the preferred employee behaviour?

* The preferred behaviour of employees accessing company data is via a secure network and a device with ant virus installed. Using a personal device can be a high risk for company data to be taken. Employees should be aware of the potential risks of a personal device to a company’s sensitive data. If an email was sent to their personal account, the employee should not open this if the sender isn’t known to them. Another way is by reading the email and seeing if it sounds like the person who has sent the message. Attachments on emails should always be treated as suspicious, more care should be taken when they see attachments in the email.
* Communications on slack via personal devices should always be treated as a risk. Sensitive information such as personal or company information, usernames and passwords shouldn’t be share on any platform. If the mobile phone was to be compromised by malware, the sensitive information could be stolen and taken for malicious attacks on the company itself or the employee. This behaviour should be adopted even when communicating via any platform.

1. What methods would you use to measure how often employees are currently not behaving according to the preferred behaviour?

* A method that would be used to measure how often employees are not currently behaving would be a phishing campaign. This would involve by either using the company’s own penetration tester or hired one to perform a complete employee survey. The test will indicate which and how many employees fall for a suspicious email and download any attachments that is involved. The results would allow the company to see what percentage of workers are aware of scams and the percentage that requires additional training.
* To help ensure employees behave according to prevent the risk of data theft, software installed on personal devices can significantly reduce the risk of data theft. However, policy must be in place for this to proceed. If the employee is against this measure, access controls on the employee should be concerned which includes weekly password resets and account management to ensure that correct behaviour is being applied. The software can manage devices to spot suspicious activity and monitor application usage. Company policies should be in place to be able to protect the sensitive data and how BYOD should be used in the work force.

1. What is the goal that you would like the organization to reach regarding this behaviour?

* A survey via email would have a preloading fake phishing attachment created by the pen testers. The goal is to get a feel of what percentage of employees identify an untrusted email to determine if training is required. Once the results have been calculated, the goal should be less than 5% that have opened the suspicious email. If the numbers are higher than the target, training would be concerned to lower the numbers.
* A policy should be in place to allow BOYD to be able to monitor the activities inside the company’s network. A goal should be in place when employed for the first time, BOYD is encouraged. However, policies are put in place to protect the company’s data and infrastructure in case of a breach. Software that must be installed to help this security be managed, software such as Mobile Device Management or Mobile Application Management tools. Passwords should always be renewed every month and a clear understanding of a termination policy to protect data been taken when an employee is terminated.

**Step 2: Involve the Right People:**

1. Now that you have a goal in mind, who needs to be involved?

* *Human Resources:*

The department is required to monitor and track the attendance of employees and the scheduling of the training that is required. The department also will give advice on the dos and don’ts when organising the required training. HR will provide the copies of the policies for employees to follow the rules on the matters at hand.

* *Finance Department:*

The Finance department involvement in this goal is to come up with the numbers that require to cover the cost of the training. Without this department, funding will not be there, and training cannot commence. The department will work closely with HR regarding the costs of training and the availability of the finance to proceed.

* *Chief Executive Officer (CEO):*

The CEO will take the strategy to the board members to discuss the security measures of the company’s data and explain the required training to try preventing a breach from happening. The CEO will explain the layout of the training, the target of the goal and any required training that needs followed up. The approval of the board is required for the funding of the training to commence.

* *Chief Operating Officer (COO):*

The COO will ensure business functions operate during the training is provided. The COO will work closely with the security team that is providing the “click bait” survey and other additional training to keep the CEO up to date with the progress. They will inform the CEO with any achievements and setbacks that may occur in the process.

* *Security Department:*

The department will develop the required method of the survey and additional training that is required. The process of the results of the outcome will be put forwarded to the COO. Depending on the results, the team will determine the risk factor and collaborate with the COO and HR to come up with a path for all employees to complete further training. They will work closely with HR to determine the details of the scheduling and delivering of the training. After the training as been completed by all employees, depending on the results will determine the next steps that’s required.

**Step 3: Training Plan:**

1. How will you train your employees on this security concern?

* *How frequently will you run training? What format will it take?*

Training will be required to be completed every 6-12 months, depending on the nature of the issue at the time. The format will be implemented over the company’s intranet where all results will be collected, and a record of employees have completed the training or has not completed the requirement.

* *What topics will you cover in your training and why?*

In the training that will provided to the employees, a while range of topics will be covered off. The following topics will be covered are:

Phishing:

Phishing will be covered in this training to make employees aware of the dangers of unknown domains. The training will cover what to look out for and education on the consequences of a phishing attack that has been successful.

Passwords:

The topic will educate the employees on how important a strong password is. Creating a strong password is important for them and the company, they should understand the risks of passwords that have been reused between personal and company accounts. The training will also cover a two-factor or multi-factor authentication system and the benefits, just for future reference when the company decides to implement this.

Ransomware:

The topic will cover “What is Ransomware?” It is important to understand the repercussions on a ransomware attack and how to prevent this from happening in the first place.

The employee will be educated why it is a most popular threat which targets businesses across the world. It will also cover the consequences on an unpaid attack and how data is unrecoverable.

Information Security:

Employees should understand that having certain access to information is a privilege. These controls required for the employees to keep sensitive information from being passed around to employees that don’t have a certain level of access.

Removeable Media:

The training on this topic will teach the employee how removable media devices such as USB’s can comprise and have an impact on security. They will understand the importance of data sensitive and why portable devices can not be used on companies assists. (If there is a policy in place)

Social Engineering:

During this subject, the employee will get an understanding what is social engineering and how they can try detecting it. The topic will teach them how to be aware of this attack and to try not to provide sensitive information and disclose this to someone they don’t know.

Physical Security:

Employees need to understand about the physical security risks in protecting areas that require privilege access. The training will educate them on issues such as piggybacking and tailgating, and how to identify these issues.

Browser Security:

Employees should understand the impotence of identifying suspicious websites and how to protect themselves. The training will cover how to keep browsers secure and up to date.

Mobile Security:

The topic will cover how mobile devices are vulnerable in the company domain. Employees will be educated on the importance on how physical security can be an issue for the company to protect unauthorized users gain access to sensitive data if the device was to be lost or stolen.

Wi-Fi:

The training will provide an understand on how Wi-Fi can be unsafe to company’s data. They should get an understanding on how a VPN works when using Wi-Fi outside the company’s secure network and how to try defending themselves against threats when working remotely.

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

The training course will be provided by a third party which will cover all these topics plus more. The training company will gather the results which will be provided to the security department. After the review of the results, this will determine how the employees are scored. The measurements of the effectiveness of the training that was provided will be in the results will indicate which employee requires more training and understanding of the security risks.

***Refers:*** <https://www.curricula.com/security-awareness-training-topics>

**Bonus: Other Solutions:**

* Indicate at least two other potential solutions. For each one, indicate the following:
* What type of control is it? Administrative, technical, or physical?

Two other potential solutions that could be adopted would be:

* Encrypt important information would come under technical forcing security measures against data theft which can not be read.
* Monitor use of computer equipment and system would come under physical to keep a record of all equipment’s software.
* What goal does this control have?
* Encrypt important information would be a preventive control.
* Monitor use of computer equipment and system would be a preventive control.
* What is one advantage of each solution?
* Encrypt important information: Encryption will convert the company’s data into a secret code before sending over the internet or into data bases. This will reduce the risk of theft or destruction.
* Monitor use of computer equipment and system: Prevents any vulnerabilities by keeping a record of all equipment software and antivirus up to date.
* What is one disadvantage of each solution?
* Encrypt important information: The software to allow this control is expansive. The employee would require upgrading to a capacity that will be able run this program. Without the required systems the operation can be compromised.
* Monitor use of computer equipment and system: This can compromise employee privacy and ethics. It could damage the relationship between employees as well.