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.

- Theft/ Loss - An employee's phone can be a target of theft from competition companies or shadow organizations that are seeking to steal data from the employee's company via their phone. Data leakage of sensitive, private, or classified work information on the personal device if it is lost, stolen, or has malware on it that is able to access the information.

-Malware itself or sketchy apps that have the potential for surveillance of work data. Many people do not even know that they may be already infected with malware on their devices, and accessing work information with an already infected device involves the potential for the malware to also spread to work networks, causing a security breach.

-Lack of Data Management, possible leak of data accessed, or too much access to data. Companies IT management won't be able to manage the content that is accessed on the employee's personal devices, and how the data may be used, and possibly for how long. With company devices, data can be wiped, encrypted, or expire access so that the content may not be left on the devices to be accessed by outside parties.

2. Based on the above 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 employee behavior would be to ask the company for a separate company-owned device that would contain its own direct VPN connection to company servers, remote access permissions by the IT department for wiping in the event of theft or loss, and features/ apps to be limited on the device so that the data being accessed could not be maliciously shared or stolen from the device unknowingly thru malware or ill intent by the employee(s). Should employees take the steps, they should have a separate "clean" device that is only used for work information and data as needed. No unnecessary 3rd party apps to be installed, or unknown recreational websites to be accessed that are outside of work-related functions. The phone should also be locked, and any encryption methods and features enabled for further difficulty for anyone else to access the phone when it is lost or stolen. Factory default "find my device" services provided by the manufacturer or service provider to be set up and enabled so that the device could be wiped in the event of a loss. Known free or paid antivirus or malware applications from approved companies can also be installed to limit potential malware when the device accesses work-related data and websites.

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.

If the solution is related to the above with a separate work device, then a device-specific secure connection network is set up on the work device, there is no need to measure if anyone is using their personal devices as they are unable to log in. However, if they are still allowed, then regular biweekly or monthly mandatory security training modules and courses should be completed by employees on a regular basis as a requirement to their regular performance or duties with or without paid incentives to be more engaging for the information to stick. A range of regular topics in many different scenarios, realistic

and hypothetical, should be presented to keep employees from neglecting the simplest of security measures with their work and personal devices.
For the ideas mentioned above, regular monthly covert tests/surveys can be performed on employees to see how likely they are vulnerable to any of the potential security risks they learn throughout their training such as attachment downloading, link clicking, phishing site(s) accessing, unknown app installing, etc. Possible required tracking apps developed by the company could also be used to report regular scan results of malware, malicious websites accessed, or other malicious data the phone may access to assess the potential threat level of an employee's device.

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.
0% should be the goal of employees downloading unnecessary or malicious apps on the devices that would be used to access work data.
Less than 5% of employees should be downloading any malicious attachments as their training should include the standard practice of double-checking the source of the sender information, the context of the email (ie if the employee asked the sender for such files or any files), and to have at least some sort of appropriate virus scanner for the device installed with features enabled to scan downloads.
Less than 5% of any employees should be clicking on any embedded email links, with reasoning similar to above, in that their regular training in their standard practices should be to perform their due diligence in checking the target of the link, asking the sender to confirm the information in the link if it was not something requested, or not click it at all.

Step 2: Involve the Right People

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

Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.
-All employees need to be involved. The first step is to have all employees at the organization on every level be involved in company security by developing a security culture with the company. Their responsibilities would range from the mundane, such as not allowing non-employees to enter secure areas of the building or access any computers, to everyday practices such as things to look for in a social engineering situation outside of work.
-IT department needs to be involved in setting up layers of security with different departments of data. HR information should only be accessed by HR individuals, company customer data should only be handled by those involved with their accounts, financial data of the company should only be handled by accounting, and so on. They should also implement firewalls, VPNs, and access portals for different data throughout the company's computer systems and devices.
-CSO should ensure that the company is implementing updated best practices and services or technology to keep up to date with utilizing security within the company across all departments. By keeping up to date with what is needed, the IT department can perform the necessary tasks to ensure company-wide security is cutting edge.
-CFO should ensure that the company's plans and budgets account for company security with separate employee devices and computers, security services both locally and in the cloud, and any other related expenses so that the company does not suffer financial losses that could be greater in the form of lawsuits and settlements. Planning for the worse is better than being faced with fixing the worse that could happen should any security measures are neglected.
-CEO should generally be involved in making sure that security within the organization is a priority. Companies with proprietary data would suffer losses from competitors if data about their proprietary

services or information is compromised and copied. Security of their financial data should be kept secret and reported as needed with required filings in order to not allow competitors or investors to distract from the company's objectives.

Step 3: Training Plan

Training is part of any security culture framework plan. How will you train your employees on this security concern? On one page, indicate the following:

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

I would like to run training on company security as a required on-boarding class to "catch up" or "crash course" a new employee about standard practices to make sure they have a universal understanding of company policies related to data security. As an ongoing event, training should be bi-weekly or even weekly requirements in smaller bite-sized modules through simple short videos, articles, and hypothetical events with 2-3 short questions to ensure user engagement to the content. Training would all be done online at employees' pace with incentives such as raffle entries for those that complete it early in order to promote the initiative in taking the training regularly.

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

The topics of the training(s) should be as follows: Malicious files, malware, password security, multi-factor authentication, website security, the importance of antivirus or anti-malware utilities, device hardware security, and best practices.

The training regarding malicious files will cover the risks that are involved in questionable email attachments and embedded file links that are to be downloaded from unknown 3rd party websites. This is an important step in attempting to protect the employees from introducing malware in the first place onto their devices.

Malware training would involve teachings about different types of potential malware that are out there, with some examples of major breaches that happened with other organizations as a result of malware. This training will also run through what each malware has the ability to do, such as key-loggers, data sniping software, hardware lockouts, draining hardware resources, along with the issues that the employee may have to deal with if such malware is introduced on their device for them and the company.

Password security, as well as MFA, will cover the importance related to stronger passwords. Why there should be tougher passwords used, not saving passwords in your browser or on a spreadsheet online, and why different passwords or password groups should be used for different types of accounts, such as email, banking, social, shopping, etc.

Website security along with antivirus utilities would cover what antivirus programs or apps should be utilized and enabled to help against accidentally accessing known malicious websites, websites that might potentially download malware onto your device, detect and prevent apps or malware that are on your device from performing and sending out data that should not be sent out or executed.

Physical device hardware training and physical access security training would educate employees on threats related to using public or free WiFi services, turning off NFC when not needed, and habits to ensure you put away your device when you change your scenario or situation. Importance would be

relayed on how public WiFi and NFC would allow bad actors to gain access to data being transmitted without your knowledge. Keeping a stronghold on your device, by keeping it with you and within your eyesight when outside of the office for meetings, lunch, etc will ensure the device is not a target of theft, or cloning when you're not around (depending on how sensitive of an organization you work for).

After you've run your training, how will you measure its effectiveness?
The effectiveness of training can be measured with reactions, improvement, effectiveness, and impact.

First, with reactions, self-assessments could be given at the beginning of the training program, or employees' introduction to the company. After their mandatory "crash course" training, a review of the things learned through a questionnaire would help with determining their understanding level, absorption of topics, and where they may need improvement.

Once it is determined what improvements are needed, training modules focused more on specific topics may be introduced into their regular training that they are required to take on a regular basis as set by the training plan.

Another review after 3-4 months with another assessment would be performed to compare the amount of improvement gained, if any, to indicate the effectiveness of the training. On-the-job performance issues that are related to areas of focus would be weighted in overall effectiveness in practice by the employee.

After regular assessment and rotation of training focuses that target weaknesses in employees, data can be compared against starting data to view the overall impact or improvements as a result of such training(s) to change and adjust as needed.

Bonus: Other Solutions

Training alone often isn't the entire solution to a security concern.

Create a security culture within the organization from the beginning and with all levels of employees from the top down. Not just individuals or employees that are involved in that sort of specific security. Guards in the front of the building or lobby should keep people out that are not authorized, or keep an eye from random loiters from stealing badges or credentials from existing employees.

Create a reward system for recognizing individuals that have a perfect security record for the quarter or year and reward them cash prizes, or raffles to company giveaways and prizes. The prizes create incentives for employees on all levels to proactively participate in security through things they've learned in training, or pay more close attention to the training in order to be able to put them into practice.