Homework 2

1. **Theft**- BYOD’s will inherently be subject to compromise to data leakage if the user access’ company servers or payroll on the devices and the device is stolen.

**Poor Policies**- If the company is required to comply with PCI, DSS, HIPPA, or any regulatory requirements, effective policy for BYODs is necessary to avoid fines.

**Malware Infiltration**- The employee uses the BYOD to access all sorts of information with the company and has access to servers, which could be breeched if a user unknowingly installs hidden malware or viruses on the phone.

<https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate>

<https://resources.m-files.com/blog/the-top-7-risks-involved-with-bring-your-own-device-byod-3>

1. **Theft**- the preferred action here would be to set up procedures in the company to plan for theft. There could be precautions to cut connection with the servers if the company is notified of the theft. There could also be multi authorization factors to be able to access the phone, with so many attempts after the phone is locked.

**Poor Polices**- Outdated or old policies should be updated at least annually in order to insure proper management of devices, have meetings with different departments to get an understanding of where the security vulnerabilities are at all levels withing the company. Ensure that policies meet to covered any requirements from regulatory authorities.

**Malware Infections**- Have trainings on how to operate the BYOD’s. In this will involve trainings to teach employees how to assess whether an email or app is possibly compromised. Develop a hotline or department for employees to ask a professional if the apps or emails are malicious.

1. In order to measure this make sure that theft is tracked within the company of all devices. Offer surveys to see how many people in the company access any work related activities from their BYOD’s. Offer free virus scans from your company’s IT department, or incentives to your employees to get their devices checked (i.e. a day off).
2. A goal for the organization to reach is 1% of the company to be subject to thievery or data leakage. Ensure malicious emails or apps are not installed or identified early on (i.e. <24 hours technical response).

**Step 2:**

1. CEO-They ae the leader of the company, in order to provide security of clients and personnel the CEO must be a stakeholder and understand the vulnerabilities of the company. They have the power to veto or pass any financial requests or needs that the company will need, needs to assess what is priority for the success of the company.
2. Management- Management needs to be involved because they are the man in the middle for the CEO and the field staff. They must be involved to learn what new policies are in place and be able to demonstrate and provide clarity to the field staff.
3. IT Department- They identify where the security vulnerabilities are within the company. They assess needs and will present a plan to help clear up these issues, possibility will have to provide a financial statement for any improvements needed. They also will provide the training for the management & provide help to the field staff and others.
4. HR Department- HR needs to be involved if the company is involved with any BYOD’s possibly for liability concerns. They can also provide information on requirements needed by regulatory authorities and ensure compliance within the company.
5. Field Staff- They are the foundation of the company and also the most vulnerable. If they are out in the field subject to theft. The field staff will often have to use BYOD’s in the field accessing the company servers, and will provide feedback to higher ups of the difficulties or issues they may run into. Also allows for a checks and balances system where the workers have a say.

**Step 3**

For the training program there will be training multiple sessions; one general assembly to update the entire company that there will be changes to the policy coming forth. Managerial trainings where management will learn how to identify threats and handle them from the management level. Staff training will be for field staff which will be allocated in training sessions online, and classes offered by the company to help detect or properly identify illicit apps and emails. These trainings will be offered in online version when physical presence is not required. The IT department will review policies on a yearly rotation, making any improvements or updating any information that could be irrelevant now. Ideally the training will take around 6-12 months for implementation with refresher courses every 1-2 years, with updated policies every year.

Topics:

1. Personnel Protection
2. What BYODs can be used
3. liability
4. Physical Protection
5. Data Protection

Personnel Protection

This is the foundation of cyber security, people matter. We must make clear throughout the trainings that no one should ever be in harms way if or during a data breach, whether that be a physical breach of the building or the theft of a BYOD.

What BYODs can be used

There would be policies in place to limit any unregistered or devices that will have a higher chance of infecting the company. This would include any self-created software’s, or hacked devices. This would be important if there are an regulatory agencies the company must abide by, because it allows for IT department to track any important data if there was a breach.

Liability

I would have training on liability concerns if there is any sensitive data that needs to be shared through BYOD’s. This is important because it will allow use to make sure our employees know their rights and possible liabilities if there ever are ever legal concerns.

Physical Protection

This would be training revolved around how to protect any equipment that is needed in field work. This would be important for situational awareness, where to leave items in the car when you must travel. This could also include self-defense training.

Data Protection

This training would focus on phishing emails, and third party app malware, and safe internet practices. Focusing on how to identify any suspicious activity you may encounter. This would also explain malware and show people in the company the different types of attacks that could be experienced.

The ways the training will be measured is through surveys, lost prevention numbers and the amount of malicious malware is exposed in the company. Offer free virus scans for BYODs to prevent and security threats and to incentivize people to get their devices checked for free.

<https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>

<https://www.google.com/search?rlz=1C1CHBF_enUS891US891&sxsrf=ALeKk00WQBidSB4bpfOVPfnZ7ZGiUrE-sQ:1624403859309&q=How+do+you+mitigate+BYOD%3F&sa=X&ved=2ahUKEwilp4X4r6zxAhVWHc0KHWp5AZIQzmd6BAgdEAs&biw=1920&bih=969>

<https://www.cioreview.com/news/how-to-mitigate-byod-risks-and-challenges-nid-20825-cid-91.html>