Bring Your Own Device and Its Impact

Deliverable #1 - Measure and Set Goals

1. Identify at least 3 potential attacks that can be carried out.

- Opportunities for data theft. Hackers will find opportunities to steal data. Evil never rests.
- Malware infiltration. User might inadvertently download an app or game with hidden malware or viruses
- Device loss or theft. Small computing devices have a greater chance of being misplaced or stolen

2. What is the behavior that employees should engage in?

- For data theft, prioritizing data protection. Some level of prioritization can increase effectiveness by seeking to only safeguard the most important assets.
- For malware infiltration, employees should attend user education seminars. Knowledge is power and the more employees know about malware and how to protect against it, the better.
- For data loss or theft, employees should make it a habit to never be out of reach of his or her device. Also, the device should be password protected. It wouldn't hurt for the user to add contact information on the back of the device with name, department, and contact information.

3. What methods would you use to measure how often employees are currently not behaving accordingly?

- For data theft, a survey should be sent/emailed to the employee every Friday asking him or her if they have secured their data on the device.
- For malware infiltration, the company should keep track of those people who are attending user education seminars. There should be check-in sheets at the seminars.
- For data loss or theft, at the beginning of each day, reception should verify that the employee is bringing his or her own device into the office. Similarly, reception should verify that the employee is leaving the premises with his or her device

4. What is the goal that you would like the organization to reach regarding this behavior?

- For data theft, there should be a zero-tolerance policy. Failure to not securing a device is irresponsible.
- For malware infiltration, within a month, all employees should have attended at least one user education seminar.
- For data loss or theft, ideally all mobile devices should be tracked every day at reception. There should be a one week grace period. There shouldn't be any problems after that.

Source: https://www.m-files.com/blog/top-7-risks-involved-bring-device-byod/

Deliverable #2 - Involve the Right People

1. Who needs to be involved?

- CEO: the CEO has overall responsibility for creating, planning, implementing, and integrating the strategic direction of an organization. The CEO also ensures that the organization's leadership maintains a constant awareness of both the external and internal competitive landscape, opportunities for expansion, customer base, markets, and so forth.

2. CSIO - the CSIO is responsible for an organization's information and data security. Responsibilities include security operations, cyber risk and cyber intelligence, data loss and fraud protection, security architecture, identify and access management, program management, investigations and forensics, and governance.
3. Front Office Manager- the FOM is the senior person in an office environment and accountable for maintaining a professional work environment, staff supervision, and administration support. The important functions of a FOM include crisis handling and office morale.
4. Security Operations Center - the SOC continuously monitors and analyzes the security procedures of an organization. It also defends against security breaches and actively isolates and mitigates security risks.
5. Emergency Operations and Incident Management - EOIM is used to support on-scene activities through the prioritization of activities and the allocation of available resources. A major function is communications between the emergency response team, business continuity team, crisis communications team, company management.
6. Reception - answer, screen, and forward telephone calls. Greet walk-in customers and other visitors and escort them to specific destinations. Copy, file, and maintain documents and records such as BYOD situations.

<Refer to the Organizational Chart at the end of this document>

Sources: https://www.thebalancecareers.com/what-does-a-chief-executive-officer-ceo-do-1918528
https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html
https://study.com/articles/Front_Office_Manager_Job_Description_and_Requirements.html
https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/
https://www.ready.gov/business/implementation/incident
https://www.careerexplorer.com/careers/receptionist/

Deliverable #3 - Training Plan

Bring Your Own Device and Its Impact

Employee training should occur once a week on Fridays. Hybrid learning would be ideal, both in-person and online. Topics to cover include:

- Clean desk policy - Sensitive information on a desk such as sticky notes, printouts, and papers can easily be taken by thieves and seen by prying eyes. The only materials on one's desk should be ones relevant to the current project you are working on. Finally, all confidential and sensitive information should be removed from the desk at the end of each working day
- Safe internet habits - Most workers have access to the Internet. For this reason, the secure usage of the Internet is of most importance. Employees must be conversant with phishing attacks and learn not to open malicious attachments or click on suspicious links. They should also understand how to disable pop-up window, as they invite risks. Finally, users should refrain from installing software programs from unknown sources, especially links infected with malware.
- Malware - A training session on malware should illustrate malware types and their implications. Malware types should include adware, spyware, viruses, Trojans, backdoors, rootkits, and such. Employees should learn how to identify malware and what to do if their device or network has been infected
- Hoaxes - The training plan should teach employees about hoaxes. Instead of trusting a hoax, employees should learn how to respond to them. Only emails that are verified by the security department and relevant to the corporate business should be trusted.
- Social networking dangers - To prevent the loss of critical data, the enterprise must have a viable social networking training program that should limit the use of social networking and guide employees with regard to the menace of phishing attacks. Also, the security department should ask employees not to provide their credentials or login information to unknown site or sites similar to the original one
- Removable media - Unauthorized removable media may invite data security issues, malware infection, hardware failure, and copyright infringement. Corporate personnel must be educated about the menaces of unsolicited removable media and prohibited from accessing any stray media such as an external hard drive, even if it's on a secure system.

Measuring Effectiveness

I would send online questionnaires on Monday (after employees attended the Friday training session) and ask the employee what he/she learned from the user education seminar. These questionnaires would then be analyzed and then filed in the Security Operations Center.

Source: https://resources.infosecinstitute.com/top-10-security-awareness-training-topics-for-your-employees/#gref

Deliverable #4 - Other Solutions

Training alone isn't often the solution to a security concern. Indicate at least two other potential solutions.

Bring Your Own Device and Its Impact

1) Hire a security guard- to enforce the BYOD policy, a guard could be hired to make sure no suspicious activity occurs at the entrance and the front desk. This is a physical control whose goals are preventative and deterrent. The disadvantage is this would cost the company some money.
2) Create an incident response plan - you could have a response plan in place as this can reduce the potential damage of a breach and allow for a relatively quick return to normal operations. Also, create a checklist of action items that should be prioritized during an attack to ensure no time is wasted. This is an administrative control whose goals are detective and corrective. The disadvantage is that it will take some man-hours to create the plan; an effective plan should be regularly tested and updated.
Source: https://securityscorecard.com/blog/six-ways-to-improve-security-posture

Organizational Chart - Refer to Deliverable #2