**Step 1: Measure and Set Goals**

1. In recent decades there has been a large technological advancement in the area of noncommercial consumer-available products. The benefits of personal devices have made it difficult for organizations to ignore the opportunities that exist by enabling employees to use their own devices to perform and meet their work responsibilities. However, as there are benefits there is also a plethora of risk. By enabling employees to utilize their devices to access private company information there exists the risk imposed by a lost or stolen device. The lack of security monitoring makes it difficult to assess the malware that exists in other applications on employee devices. Additionally, there are privacy risks created due to the inability to control who is accessing the information when there is no control of the people in the environment. Potential attacks include malware attacks from lack of protection on applications such as phishing attacks from emails received. Users are also prone to social engineering and packet sniffing by a lack of network management.
2. Considering the risks it is imperative that employees behave in some preferred manner. Preferred behavior would include compliance regarding the installation and maintenance of security software on their devices. For example, installing anti-virus, using VPN encryption, and using company cloud storage. Another preferred behavior would be for employees to make it a habit to maintain a strong password for protection on devices and networks. Lastly, employees should also take physical measures to ensure devices remain locked and are reported if lost or stolen. All such details should be outlined in a detailed BYOD policy that is agreed to be adhered to by the employees participating.
3. To measure how often employees are not behaving according to the agreed upon standards would require compliance testing. There are various ways to test employee’s behavior and some of them were discussed during lecture 1. For example, hiring a pen tester to run a phishing campaign on the employees. The result from the phishing campaign could provide insight regarding the percentage of employees who downloaded the malicious files versus those who complied with the policy set. Another example would be to use available commercial software to monitor location and information retrieved from the company database. The purpose of using location would be to understand where employees are working. Working in a public setting might go against the policy. By monitoring the information retrieved would be to ensure that workers are accessing on a need-to-know basis.
4. As discussed during lecture, a business goal is always to increase the bottom line. Often these goals do not go hand in hand with the IT security goals. By Silvercorp choosing to incorporate a policy that enables employees to use their own devices, the results should be more gainful than wasteful financially. Silvercorp could set goals for employees. For example, only 10 percent of devices should result in being lost or stolen. Ideally, zero loss would be the best but such a number is unrealistic. In an article by Phil Muncaster he points out that the UK government lost 300+ devices since 2018. Performing more research, it becomes obvious that lost or stolen devices are an upward trending problem. Another goal would be to have less than 5% of employees downloading suspicious email attachments from that phishing campaign done by the pen tester. Last goal would be that all employees’ logins contain strong password.

**Step 2: Involve the Right People**

In considering who would be involved in the planning and initiating of this policy. It is important to consider who is responsible for implementing this new strategy, who will be affected by its implementation, and finally who will be required to monitor it after its deployment. Below is a list of individuals whose roles are vital to the process of incorporating this new policy.

* The Chief Executive Officer (CEO) is responsible for overseeing all operations within the organization. The CEO is reported to by departmental chiefs. It would seem important to at least involve the CEO of this plan to enable workers to use personal devices.
* The Chief Information Officer CIO is one of the C-level officers who report to the CEO and potentially the Chief Financial Officer (CFO). The CIO is a leadership role responsible for the Information processing systems being utilized by the organization. By Silvercorp enabling employees to use their device (BYOD), the CIO is responsible to find solutions, and set policies for devices to work seamlessly with the organization software to enable workers to perform their responsibilities. The CIO views implementation as an investment.
* The Chief Information Security Officer (CISO) would also need to be involved in the development of this plan. CISO typically reports to the CIO and is responsible for reducing cyber threats and ensure data is securely protected. They play key roles in creating policies and security architecture to meet organizational needs. The implementation of a BYOD policy significantly increases the potential threats that exist to the company. Silvercorp CISO would be able to assess the threat landscape and make plans to better mitigate the risks.
* The IT Manager is someone who reports to the director or CIO. They are responsible for the system performance. They are also responsible for the implementation and maintenance of the current system. They are responsibility is to ensure that all employees using a company system can achieve their responsibilities. They are responsible for modifying and determining new information processing systems.
* The role of an Engineer is responsible for the development. The receive direction from management and postulate and develop methods to meet those requests. The BYOD implementation by Silvercorp is developed by the engineers. The engineers create a plan and pass to the administrators for execution.
* The role of an administrator is a responsibility for the day to day activities. They are responsible for ensuring that day to day tasks running. For example, a security administrator is responsible for monitoring and for resolving security alerts.
* IT analysts are at the bottom below the administrator. There are various types of analysts ranging from IT, Security, networking, etc. They are responsible for assessing and monitor the internal and external aspects of the IT systems. Analysts grant access while providing solutions to employees.

**Step 3: Training Plan**

By training employees an organization can ensure that the level of awareness is equal throughout the company. When enabling employees to participate in using their own devices to perform work duties, it is important that training be incorporated to make employees aware of the risks and the correct behavior to achieve success. Training should be held annually and as well for newly hired groups of employees. It is important to start when employees are hired because it can make them aware of issues that are faced on a day-to-day basis. The initial training for new hires should be in-person alongside their other training. This is to ensure that if there is any confusion, then feedback can be immediately provided. If an employee is past the training phase of their employment, they should participate in the online training that takes no more than two hours of a working day. The training should conclude with a mild test to ensure that there is a level of comprehension that has been attained by participating in the training activity. The training should be mild enough to equip employees with a general understanding of the threats that exist, and the behavior required to protect themselves and the company resources.

When training Employees about using their personal devices to perform work duties, employees should be taught about the value-added to the organization. Employees should be taught about the types of devices, software, and application that are supported. Thereby ensuring that company software works appropriately with the system brought by the employee to perform their duties. There should be topics regarding reimbursements and stipends of lost or stolen devices. Other important topics would be regarding the security policies for networks, passwords, privacy, and data ownership policy. The training should also provide the employees with information regarding how to troubleshoot and-or how to escalate problems. It is also essential that the employees are made aware of the threats that exist and the potential situation that they may be presented with. By training and educating employees with this knowledge, employees are properly made aware of the expectations set by management.

A test or quiz that has a mix of questions would be beneficial towards measuring the effectiveness of the training. The test would cover all topics of the training. In addition, there would also be situational questions to see how employees apply what they have learned. The testing would require that employees receive a certain grade in order to participate in bringing their own device. In addition to tests there could be surveys done to see how educated employees were prior to training and post.

**Step 4: Other Solutions**

Administrative controls could be created to ensure that employees are behaving as required. For example, the separation of duties would be a preventative control. The goal of this control is to reduce the ability of one employee to have full capability to complete a task. An advantage is that if a device is compromised, the attacker is limited in their ability to damage the company. The disadvantage is that an employee cannot fulfill the entirety of a task. Data backup is a corrective administrative control that can be implemented for lost, compromised or damaged devices. Technical control is implemented through the system. An example of a technical control would be encryption, firewalls, and least privilege. Encryption for example is a preventative control because it protects confidentiality of data transfer. The advantage would be that decryption is very difficult and therefore data transfer on a network is made safe. Least privilege is another technical control which is beneficial because employees have access to information on a need to know basis. The disadvantage is that scalability of a job role is slowed down due to the lack of access.