**Chadwick Spencer**

**Unit 2 Homework**

22 September 2020

**Step 1: Measure and Set Goals**

1. Some potential attacks that could be carried out as a result of Bring Your Own Device (BYOD) practices are:

* Phishing attacks
* Ransomeware
* Malicious apps (Malware attack)
* Password attack
* Eavesdropping
* Data loss

1. Desired behaviors for employees using their own devices for work would include the following:

* Employees shall only open email from verified, trusted, and known sources.
* Employees will only download and open attachments from verified, trusted, and known sources.
* Employees shall only connect to company email via a VPN.
* Employees will not jail-break their devices.
* Employees shall keep their device OS up-to-date with the most current OS version.
* Employees shall encrypt their devices.
* Employees shall keep their devices secure (on their person or in a controlled location) and shall notify IT of any lost/stolen devices and will take action to disable any missing devices not located within a 24 hour period.
* Only employees shall use their devices.
* Employees shall only communicate via Slack while on a company VPN.
* Work related applications shall only be downloaded from verified and trusted sources (company app store, iTunes, Google Play).

1. Methods used to measure how often employees are currently not practicing the preferred behavior could include the following:

* Surveying employees to determine if other family members ever use their devices.
* Surveying employees to determine how many jail-break their devices and how often they update their operating systems.
* Monitoring network traffic for IP addresses, source and destination ports, timing of data/packet transmissions for irregularities.
* Surveying employees to determine if they download suspicious email attachments.

1. Reasonable goals would be:
   * Less than 5% of employees losing devices.
   * At least 95% of employees have the most current OS update.
   * No jail-broken devices in the organization.
   * 95% or more employees using a VPN for communicating with work servers.
   * No employees reporting other family members using their devices.
   * 95% of employees have encrypted devices.
   * No irregular network traffic.

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

* **CISO** - The CISO will own the corporate security posture and will focus on the corporate risk tolerance. They will report the risks of the BYOD policy to the Board of Directors and will ultimately guide the cybersecurity efforts to minimize and monitor mitigation efforts.
* **CIO** - The CIO will own the technology required to monitor, analyze, and mitigate devices participating in the BYOD program as well as the threats they actively pose. They will report the infrastructure needs of the IT and Security teams to the Board of Directors.
* **IT Manager** - The IT Manager will ensure the appropriate tools and methods are deployed on the corporation’s network as prescribed by the CISO and the CIO. They will be responsible for the daily operations and integrations of networks and devices.
* **HR** - HR will ensure that the steps taken to monitor the BYOD program and the steps to mitigate risks posed by the BYOD program do not place the corporation in a state of jeopardy by infringing on the rights of employees. HR will likely vet any surveys and employee requirements to participate in the BYOD program to ensure no rights are violated and to protect the company.
* **Legal Counsel** - Legal Counsel will ensure that no state or federal laws pertaining to data governance as well as data privacy, of clients and employees, are violated by the BYOD program or the actions taken to monitor and control the BYOD program.
* **Security Analysts** - Security Analysts will be responsible for the day-to-day monitoring of the devices and any associated impact they may pose. They will run the tools and monitor traffic over the network to detect any malicious software, malicious files, and any abnormal network traffic and data transfer.

**Step 3: Training Plan**

**Training Frequency**

Training for the BYOD program will consist of both in-person and online training depending on the time of the training cycle. Training will occur at the following times and frequency:

* New Hire Training

New Hire Training will occur in an online format for each new hire as a part of the onboarding process. Upon completion of the online training the new employee will review the training with the IT staff establishing their accounts and access.

* Existing Employee Training

Existing Employee Training will occur in an online format for a 90 period to ensure all current employees are covered under the program. There will be additional review of the policy during device enrollment and account connection.

* Refresher Training

Refresher Training will occur on an annual basis in an in-person format. The training will be held in classes during the months of July and December to cover employees with hiring anniversaries between January - June and July - December, respectively. Training opportunities will be available for two weeks during July and December to ensure all employees are trained. Remote employees will have the opportunity for training via a simultaneous web-cast to ensure consistent delivery.

**Topics to be Covered**

Topics to be covered will include the following:

* Benefits of BYOD  
  There are numerous benefits of BYOD policies for both the employees and the company. It is important for the employees to understand how using their own devices will contribute to their work satisfaction and productivity through using familiar devices.
* Risks of BYOD

Employees will be informed of the risks posed to SilverCorp by extending the BYOD privilege. Risks to be covered will include:

* Phishing
* Malware
* Data breaches/loss
* Lost devices
* Ransomeware

* Acceptable Use

Employees will be presented with acceptable uses of their devices and will understand the potential compromises and risks posed to SilverCorp if acceptable use is violated.

* Supported Devices  
  Employees will be presented with a list of supported devices and minimum operating system requirements so they will know if they are currently eligible for the BYOD program. Only devices in the supported devices list will be allowed and exceptions can only be made with prior approval by the IT manager.
* Reimbursement

Employees will understand the reimbursement paid to them as compensation for SilverCorp’s benefit for the use of their personal devices. This will encourage program adoption and will ensure that employees obtain approved devices.

* Security

Employees will understand and accept the increased security measures that may be applied to their devices in order to protect SilverCorp data and infrastructure. This will be a condition of participating in the BYOD program.

* Risks/Liabilities/Disclaimers

Employees will understand the risks presented to them should their devices become compromised or lost. They will understand the importance of backing up their personal files and information so they will retain access should their device become lost, corrupted, or otherwise compromised.

Effectiveness of the SilverCorp BYOD training will be measured by following:

* Conducting employee surveys to interpret user behavior with a goal of 95% compliance. This will provide insight into the number of employees with jailbroken devices, email attachment behavior, website visitation practices, network connection practices, device sharing practices.
* Network traffic will be monitored and compared to an accepted baseline established prior to the initiation of the BYOD program. The goal is to see less than a 5% increase in abnormal and suspicious network traffic after program initiation.

**Step 4 Other Solutions**

Other potential solutions include Mobile Device Management (MDM) and Mobile Application Management (MAM).

Mobile Device Management (MDM)

* This is both technical and an administrative control.
* This can be both a detective measure and a preventative measure in which IT administrators will be able to centrally manage all allowed devices through the installation of MDM software on employee devices and track activity.
* An advantage of MDM is the ability of IT administrators to employ password policies, perform remote data wiping, and network monitoring for all enrolled devices.
* A disadvantage of MDM is that they can pose privacy issues through company monitoring of personal employee assets.

Mobile Application Management (MAM)

* This is both a technical and an administrative control.
* This is a preventative measure permitting access to company networks and data via the use of specific applications that are developed and/or controlled by the corporation.
* An advantage of MAM is secure data access by mobile devices via corporate applications.
* A disadvantage of MAM is that it does not aid in detecting or blocking shadow IT, therefore allowing workarounds to some access inconveniences.