**Sidney Robinson - Unit 2 Homework**

* Scope
  + BYOD – Bring Your Own Devices
  + There is a current movement by corporations to employ BYOD for their employees.
  + 60% of organization currently allow employees to use personal devices for work purposes, 26% of organization do not allow BYOD, and 14% have no plans to allow BYOD
  + BYOD represents a challenge to protecting an organization's infrastructure. Imaging all the different devices and operating systems that you’ll need to harden and protect the corporate network and applications against, to allow users to use BYOD devices. Then why do organizations allow the use of BYOD devices? Here are the reasons:
    - Advantages;
      * BYOD helps employees to be 74% more productive
      * On average 57 minutes of productive time is reclaimed
      * BYOD represents a cost savings in purchasing, supporting, distributing, and end of use processes of these type of devices
      * 58% of employees have opined more satisfaction and productivity as realized benefits in surveys about their use of personal devices to do company work.
    - Disadvantages;
      * The biggest security weakness in an organization is the system users. This then is multiplied by the number of BYOD devices that they are allowed to use on the network.
      * Personal and corporate credential security must be properly protected and monitored?
      * Sharing corporate information with the introduced devices adds further exposure to malware, spam, ransomware, and other attacks.
      * Each device must be properly secured and information will need to be protected when the user is accessing the corporation’s network, applications, and corporate information
      * BYOD devices represent an almost 50% increase in the possibility that an organization may have a data loss incident. Lose the device, possibly lose information, or open the organization to data loss attacks.
* Known Threats
  + Device loss or stolen
  + Insider threats
  + Organized cybercriminals
* Possible Points of Attack
  + Devices lost or stolen can give bad actors access to stored user and corporate information. This information can then be used to access and compromise the organization
  + Employees who are sharing their personal device with the organization they work for will often knowingly create a cyber security risk. Perhaps by carrying infected devices into corporate zones that bad actors would normally not have access to, or perhaps by not properly securing their device with passwords… Perhaps by accessing the network with a device that has been infected
  + Phishing and Malware attacks will inherently gain more points of attack, because these devices have not been the focus of corporate level security. Bad actors are now trying to utilize BYOD devices because they can be overlooked by Corporate IT and present a powerful platform to attack from.
* Vulnerabilities
  + Corporate leadership, employees, and IT assessment, training, and understanding of Cybersecurity as it pertains to BYOD devices.
  + Increased risk and exposure to Malware and Phishing attacks due to the introductions of multiple BYOD devices and their operating systems
  + Preparation for BYOD incidents
* Risk
  + Using BYOD devices will increase the organizations exposure to Data Loss incidents by 50%. This is an unacceptable level of risk and should be mitigated.
  + It will be imperative that accepted BYOD devices be monitored and protected when connected to the corporate network, this would include user authentication, user data authorization, and data encryption.
  + BYOD system access will need to be closely monitored to identify when threats and attacks exist. Systems must be put in place to respond to attacks by bad actors, and also to respond to BYOD loss or stolen device incidents.
  + 41% of organizations experienced Data loss incidents in 2013, a 50% increase in this probability was experienced in 2015. The exposure to data loss due to BYOD devices is palpable. We will need to establish governance, training, and hardened IT systems to protect the organization and reduce our exposure to this type of data loss to below 20%.
* Risk
  + **Recommendation:** Accepted BYOD devices must have an IT vetted virus/malware protection software installed and running when accessing the corporate network. This software must scan the device prior to connecting. When the device attaches to the network, the device's scanned status must be reported prior to further authentication. When the device is found to be infected, IT should mobilize a response. Please note: this initial connection should be done in an isolated server environment to protect the corporate network and give the CSOP’s response teams a safe place to respond and work.
  + **Recommendation:** Connection to the corporate network should be done through a VPN and Encrypted architecture to further protect the exchange of data.
  + **Recommendation:** An application gateway should be created for download and install on the accepted BYOD device. This application will allow us to update and harden access points as necessary.
  + **Recommendation:** Training, training, training. The exposure to hack and data loss created by BYOD devices must be identified and demonstrated. Leadership, IT, and employees must be trained again and again on the seriousness and risk that is presented by the privilege to access and work with corporate data and applications on their personal devices

References:

***EVERFI*** *- h*[*ttps://everfi.com/blog/workplace-training/cybersecurity-how-to-reduce-the-risks-of-personal-devices/*](https://everfi.com/blog/workplace-training/cybersecurity-how-to-reduce-the-risks-of-personal-devices/)

***Wharton U of Pennsylvania*** *- https://knowledge.wharton.upenn.edu/article/mobile-devices-and-cybercrime-is-your-phone-the-weakest-link/#*

***HEIMDAL*** *-* [*https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/*](https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/)

*https://heimdalsecurity.com/blog/byod-security*/