Taylor Norman

Assessing Security Culture within Silvercorp

Step 1.

Bringing your own device (BYOD) has become a very common trend among businesses, although along with the convenience there is an added level of risk involved. Due to the combination of using a device for everyday life and business needs there is a much greater risk of falling victim to multiple types of attacks or hacks that could end up affecting the company.

The first risk that comes from using your own device is the threat of Malware. Because there is the potential of an employee downloading all sorts of information from the web or clicking on suspicious email attachments, there is the chance the download may contain hidden malware which can be transmitted into the company network the next time they connect.

The second risk that is very likely with BYOD is the potential of the employee losing their device. This can lead to a leak of confidential information which may have been stored on the device either in texts, files, or emails.

The third risk of BYOD is the risk that comes from the employee connecting to an unsecure Wi-Fi network, where they risk exposing information to hackers looking for opportunities to steal data from unsuspecting victims.

Due to the three risks I have listed above it is important that employees using their devices for both work and personal use do not open attachments from unknown sources. They should not use unknown and unsecure wi-fi networks while transferring data and they should not download unknown applications and files onto the device which may have potential to contain malware. All devices should also be set up with password protection as well as a find your device tool which can either wipe or find the device if lost or stolen.

In order to test that employees are following these policies the company will first ask employees about their device usage including if they download from unknown sources and open unknown email attachments. The company will hire a third party team that will send out “phishing” emails that contain attachments and we will track how many employees open them. We will also create a password policy requiring employees to create a strong password and change their password monthly. The goal is to get 100 percent of employees to either use a password or fingerprint lock on their device, and to get less than 3 percent of employees opening unknown attachments. Our goal is to get less than 5 percent of employees to use wi-fi from an unsafe source.

Step 2. Involve the Right People

Human Resources must be involved during this process. It is important that HR participates in scheduling training times and dates to achieve 100 percent employee security awareness training participation. They will also be important to ensure no employee rights are being broken during the process.

The Law department will be important for understanding the laws and policies the company must follow in order to best protect the company.

The security team must be included because they will help with developing the policies based on BYOD security. They will work with HR to provide training on scheduled days. They will also help with setting up access controls, ensuring employees cannot access files on the company server which they are not authorized to access.

Employees will be involved because they must be able to participate in the training. They will be the ones with the devices, and it is important they receive full training surrounding the risk of using their own devices and how they can introduce malware to the company network.

The C-Suite should be involved with the other teams to guarantee board and management support has been achieved. It is also important that they procure the funds necessary to implement the new policies and training procedures.

Step 3. Training Plan

In order to ensure training throughout the entire company we will have 25 percent of employees attend a quarterly training in person, until 100 percent of employees have completed the training. Before the training begins it is important to have a starting number on the percentage of employees opening unknown attachments, so the security team will send emails to everyone to get the starting number. After each group has been put through the training the team will send emails to see the new numbers of employees who still open the attachments. This process will repeat itself until all employees have been tested post training. If an employee continues to open an attachment from an unknown source after training they will be sent through training again and given a stern warning about future consequences for non-compliance with company policy. Continued training will be held through an online session where they must complete a course once a year to renew their knowledge and update them with new risks and policies.

The training will cover the topics of malware and phishing and the risks it presents to both the employees devices as well as how it can spread from their device to the company network. There should be a mixture of a slideshow and a lecture by the security team. After the employees understand what malware and phishing is we will transition into how opening unknown attachments, and downloading from unknown sources can spread malware and how they should avoid doing these things to protect themselves and the company. Once we have explained the reasoning behind the policy we will have employees read over the new policy developed by the security covering phishing and have the company sign an agreement to follow the new policy.

The next step in the training will help to understand what a Man-in-the-Middle attack is and the importance of only using secure networks. We will be sure to include options to better protect information if the employee must transfer data over an unsecure network. This will include how they should take steps such as using a vpn to help encrypt their data. The training will end with a final presentation about the importance of a strong password and why it should be changed often and is mandatory on their devices for work purposes.

Because training alone is never enough to completely prevent damage to the company the security will implement the policy of least privilege. This will protect confidentiality of information by protecting it from access by unauthorized employees. This control will be a technical control that is preventative because it will ensure that employees will never have access outside of their level of clearance preventing private or protected information from getting into the wrong hands. The disadvantage that comes with this is as employees find they cannot access files they need they will be required to contact IT with a request to gain access, which can slow down productivity. Overall the measure will have more of a benefit that a disadvantage when considering company security.

Hollander, G., 2019. *The Top 7 Risks Involved With Bring Your Own Device (BYOD)*. [online] Available at: <https://resources.m-files.com/blog/the-top-7-risks-involved-with-bring-your-own-device-byod-3>.

Ogden, J., n.d. *The 7 Scariest BYOD Security Risks (and How to Mitigate Them!)*. [online] Cimcor.com. Available at: <https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate>

Digital Guardian. n.d. *The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits*. [online] Available at: <https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>