***Homework Assignment Module 2 Brenda Schecher 12/8/2022***

***Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.***

The latest trends is companies allowing their employees to work from their personal devices. BYOD stands for Bring Your Own Device. According to Leaders Choice staff report, there are five main security threats posed by BYOD (leaderschoiceinsurance.com, 2019, Leaders Choice Staff); Loss or stolen devices, malware, friends and family, link to the cloud, and security breach.

Loss or stolen: Organizations can be at risk of a security attack if the employee’s personal equipment is stolen. The criminal could access the company data from the employees phone or laptop.

Malware: Juniper Networks reported a 155% volume increase from 2010-2011 of malicious software on mobile devices (leaderschiceinsurance.com), hence having data on personal device would jeopardize the company sensitive data from being breached.

Friends and family: having access to personal devices impose a risk of sensitive data being compromised as well. A report by the U.S. Treasury Department’s Financial Crimes Enforcement Network found that in 27.5% of suspicious activity reports filed by depository institutions between 2003 and 2009, the identity theft victim knew the suspected thief, who was usually a family member, friend, acquaintance, or an employee working in the victim’s home (Leaderschoiceinsurance.com, 2019).

Security breach: if a security breach occurs, your company could receive civil penalties and open the door to litigation if employees have personal information stored in their personal device.

***Based on the previous scenario, what is the preferred employee behavior? (For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.)***

Deciding which individuals are permitted to using personal devices and which type should be established. Excluding senior manager whose data is more sensitive could be a solution as well. Another option would be to exclude personal devices all together. This might be difficult as many more people are working from their home offices.

If personal devices must be used, the company could implement policies around the BYOD device such as ensuring the company has access to the data within those devices for record retention and litigation purposes & ensuring there is a VPN connection and anti-maleware software installed.

Ensuring employees are trained on latest security policies and best practices will help reduce malicious software from being installed.

***What methods would you use to measure how often employees are currently not behaving according to the preferred behavior? (For example, conduct a survey to see how often people download email attachments from unknown senders.)***

Integrate risk management and train employees on the policies. After implement and training, the company could conduct quarterly or yearly assessments by sending out fake phishing emails to see who click on the links. Use the tool as a learning tool to make employees aware issues and promote preferred behavior.

***What is the goal that you would like the organization to reach regarding this behavior? (For example, to have less than 5% of employees downloading suspicious email attachments.)***

Having a goal for zero tolerance of downloading suspicious downloads or visiting unsafe websites is unrealistic as everyone is human and make mistakes. Having a goal of less than 5% is realistic and could be manageable by implementing ongoing education and training for employees.

***List at least five employees or departments that should be involved. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.***

**CEO or owner**-Its very important to have the owner or CEO support the new policies by ensuring there is money budgeted to mitigating security risk. Perhaps new equipment or software will need to be purchased as well as company time for training. Support and communicating companywide about the initiative will help improve employee buy in.

**CIO**-its important the CIO communicates the direction and budget to the managers within IT to help with discovery of tools and training programs.

**COO**-need to communicate the changes to the various departments within the company. Training the teams against security threats will be imperative with this role.

**Senior security managers** will need to ensure proper security tools and monitoring is in place by training analysts and other IT staff.

**HR** will need to be on board as well since this area is usually responsible for training new hires. All new hires should go through appropriate security training.

***How frequently will you run training? What format will it take (e.g., in-person, online, a combination of both)?***

New hire training programs will be critical to have new employee behavior expectations in place around the company’s security framework. Initial training should be done in person with all employees, including new hires, while follow up training can be done remotely on a quarterly basis.

***What topics will you cover in your training, and why? (This should be the bulk of the deliverable.)***

After the company had completed their risk analysis and understand and agree on the company’s most valuable assets, the company can then decide on how they want to move forward with the BYOD policies and train accordingly. Topics should include how as an employee is their responsibility to ensure the data and systems remain secure. Communicating policies and regulations in which the BYOD device will affect around security issues is imperative as the company data should be handled properly. Making sure the employees are aware of bad behaviors like clicking on links or reusing their credentials can open the door to attacks. Education them on topics such as how to prevent data from potential attacks such as ransomware, phishing emails, SQL injections and DDos attacks. The employees should have a list of folks that they can contact if there are questions about their application or device.

***After you’ve run your training, how will you measure its effectiveness?***

After running training, sending out surveys and quizzes to test the knowledge of the content covered in class would be beneficial. This will help determine if extra training is required for employees.

Another measure is sending out phishing emails to see how many employees click on those links. Determine if the amount is decreasing or increasing. If increasing, perhaps additional education is needed. Another good tool is to reward and give shout outs to employees that are doing a great job with security. If they ask questions raise their hand when they need help, question suspicious activity, and help train other team members, perhaps they can win a new car. (Just kidding). Perhaps a gift card or reward would help foster positive behavior.

***List at least two other potential solutions. For each one, indicate the following: What type of control is it? Administrative, technical, or physical?***

***What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?***

***What is one advantage of each solution?***

***What is one disadvantage of each solution?***

Changing the application itself and ensuring that its more secure with BYOD devises is an additional solution. This would be an administrative control. This would be preventive as it will help ensure the data is secure in the application. Advantage would be not having to supply so much hardware to the employees and to retrieve when they leave the company. A disadvantage is ensuring all data is secure in the event of employee leaving company or in event of loss device.

Another potential solution would be to require MFA or two factor authentication. This would be a preventive goal as it will help ensure safety when the employee is using their BYOD to access applications. This would be a technical control as this will help stop future attacks or actors attacking the application and/or network. Advantage would be to add extra security a possible disadvantage to this would be its more time consuming for the user.