Week 2 Homework: Assessing Security Culture

Step 1: Measure and Set Goals

1. **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.**

There are many unique and distinct security risks to companies/organizations allowing employees to utilize their personal device(s) to access work information whether they are public or private. Employees enjoy the ability to keep track of one device and convenience of managing their personal and work lives on one device. However, the risks/attacks become much more apparent with advances in technology on almost a daily basis and with so many different entry points into company/organizations systems.

For instance, if a critical security patch isn't completed on a personal device or the employee is using an unsecured network, how ready and prepared is that business to deal with the potential attacks or risks. Employers must outweigh the risk of personal convenience, morale, productivity and happiness or the potential security risks to the company's computer systems. Tom Tovar, CEO at Appdome says, "Mobile hackers have discovered that 85 percent of mobile apps have little to no protection, which allows the criminals to continuously harvest data, connections, resources, and infrastructure from mobile consumers and mobile businesses by targeting these unprotected mobile apps. In the past, hackers spent most of their time on the mobile infrastructure. Today, hackers can easily find an unprotected mobile app and use that unprotected app to design larger attacks or steal data, digital wallets, backend details, and other juicy bits directly from the app." https://technologyadvice.com/blog/information-technology/cybersecurity-trends-2020-byod-mobile/

The three attacks that I feel are risks that SilverCorp needs to prepare for are:

1) Opportunities for Data Theft through lost or stolen devices

   According to ccb Technology, over 60% of network breaches are due to a lost or stolen device. This would be your worst-case scenario because a single missing device containing sensitive data is enough to jeopardize the entire business. Therefore, it is critical that devices are protected with a passcode, facial or fingerprint recognition. It is also important to have countermeasures put into place such as remotely wiping a device as soon as it is reported missing or stolen. https://ccbtechnology.com/byod-5-biggest-security-risks/

2) Malware Infiltration

Malware seems to be one of the biggest threats that comes when it comes to employees utilizing personal devices in the workplace. These malicious apps can really damage mobile devices, which in turn can infect a whole companies computer system and networks if that software is introduced with BYOD’s. Employees can unwittingly download a malicious app(s) or visit malicious site, where sensitive data can be grabbed and can cause massive data breaches. This is not typically done on purpose by the Employee but with a BYOD policy and can and does happen because there aren’t firewalls set-up, security patches that are utilized on workplace devices, etc.

3) Unsecure networks

These unsecured networks, such as public Wifi networks, leave users vulnerable to man in the middle and phishing scams which can result in data leakage and the employers security being compromised. Especially in our current times, home networks for remote workers can also be a great concern for employers as unsecure networks/Wifi are easy targets as they are usually shared with multiple items including gaming consoles, TV’s etc.

2. Based on the above scenario, what is the preferred employee behavior?

The preferred employee behavior(s) based on specific risks and security issues for employers would initially be to make sure that they participate and complete all training for Cybersecurity and fully understand have read the BYOD Policy that for the employer. Based on what I have seen from employers, this would initially be completed during onboarding then based on the everchanging environment within technology and security issues.

Once training has been completed during the initial onboarding based on the risks I mentioned above, I would recommend the following for the employee behavior:

a) If device(s) are lost to report to the employers’ security team and the manager immediately. This will enable the team(s) to do what they to do to make sure the data is not at risk.
b) Follow all rules enacted by the BYOD Policy most likely including keeping all software up to date, utilize strong passwords with long, unique and random passwords; not utilizing blacklisted sites from the employer, always back up the device(s), and if available through the employer utilize device encryption. If something is downloaded, you may think it was blacklisted or for any other reason fell you have been compromised discuss it with your manager and let them decide the next step.

c) Make sure that the VPN is being utilized when working from a BYOD if available from the employer, if not, make sure that you are always utilizing a Secure Network approved by the employer and that you never utilize a public WiFi or chargers in public places. If you do accidently utilize an unsecured network report immediately to your manager what occurred and then allow the employer to take care of the issue.

3. **What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?**

It would be important to audit on compliance and security for all employees on a cycle, that will depend on the number of employees within SilverCorp. This will help mitigate risks associated with a BYOD policy and usage. When the audit does show that issues have been found; training(s) would be required in order to continue utilizing the BYOD, however, if these issue(s) were to continue SilverCorp would remove the ability of that specific employee(s) to utilize their own device and would either have to rely on the SilverCorp's devices or look for a new job.

There would be an Audit Checklist that would be developed by the Security team that all employees would have access to so they would be aware of what the team would be looking at when their device(s) are audited. The checklist would be developed specifically for SilverCorp and their specific environment; it would not be a canned/template checklist and would be a living document that would change as needed. Some of the key pieces of the checklist would be:

- To review all sites that are being utilized and visited over the time period being audited.
- Make sure are utilizing the VPN system put in place by the employer; they are required to log into the VPN system during their work period. This would be monitored by checking timesheets with VPN access.
- Make sure they have attended all security trainings and signed off on and participated in the activities associated with the training.

However, I do feel that training is the key and should always be the initial step. The training might be a little different than an employee who is struggling following the rules that those that do. It can be difficult to tell individuals how they can or can't utilize their own property, but they have to be trained to understand the need and importance of the security rules that are in place.

4. **What is the goal that you would like the organization to reach regarding this behavior?**
    - We would hope that we have 97% of employees that are utilizing the VPN system while utilizing their BYOD's at all times.

- We would hope that no more than 98% of employees are telling their managers who then will share with the Security team when a device(s) are lost or could have been possibly attacked.
- We would have that less than 95% of our employees are following the BYOD Policies and adhering to the trainings they have been through and the documents they signed to show their support for the BYOD and what they learned.

Step 2: Involve the Right People

Now that you have a goal in mind, who needs to be involved?

The Departments that need to be involved are:

- C-Level Executive Team from who the Technology/IT/Security Division will need to work with frequently to keep the SilverCorp Network secure. This would most likely involve the:
    - CEO as they need to be aware of what is occurring within SilverCorp at all times.
    - CSO as they are ultimately responsible for the security for SilverCorp including the BYOD Policy and keeping the company safe from risks.
    - CIO as they are responsible for establishing all the networks and maintaining the internal workforce devices.
    - COO as they are responsible for all the goings on within SilverCorp including HR, Marketing, Finance, etc.
- Human Resources Department
    - Work with onboarding, training and the security culture that will be engrained into the SilverCorp employees.
    - Work directly with those who are breaking the rules and working within the parameters established including the consequences.
    - Will establish information meetings, round table discussions, Q&A sessions etc.
        - This will assist employees in better understanding the reason for the policies and procedures for the BYOD rules and the security issues and risks that can occur. As the Security Culture and Audit Tools are living documents they do and will change, and employees need to be kept informed.
- Marketing Department
    - They tend to understand how to communicate with the public and employees better than the IT and Security Departments)
    - They will establish guidelines, emails and templates and be prepared with what to do (game plan) in certain circumstances to help mitigate issues that do arise that could impact SilverCorp.
- Ambassador Team (established during the creation of the Security Culture)
    - This team would involve a high, mid and lower management individual from each of SilverCorp's Departments within each division who will meet with a manager from the Security and IT Departments.
        - They would meet once a month virtually to discuss issues that have arisen within their teams with the BYOD Policy including the use of blacklisted apps, software, etc. They will also provide concerns that employees have to the table for the CSO and their team to understand and to policy to enhance the Security Culture.

        - Then each department would then have a lead that would report quarterly where each division representative will meet with the CSO and their team to discuss behaviors, enhancements that will need to be made, etc.

- All Employees
    - They need to have motivation to have a buy in to the BYOD Policy. Which requires them to listen, learn and participate in activities that are created to assist in guide them to successfully understanding and utilizing their own devices within SilverCorp.

https://securityculureframework.net/the-organization-module/

Step 3: Training Plan

The trainings would be biannual trainings via an online training environment with small groups with employees from each division and department. The trainings would be engaging, and bite sized. Regular training for Security risks is critical to the success of any organization were BYOD is being utilized. The small groups will engage as well as make the experience fun and exciting for them to retain the information that is being shared with them.

As mentioned above there will also be information sessions, round table discussions, Q&A's and a variety of small sessions to help guide and assist employees in better understanding Cybersecurity and the BYOD Policies within SilverCorp. This would not be required but employees would be allowed to attend during work hours. They would typically be between ½ hour and an hour held once a month in a variety of locations and times within SilverCorp.

A training schedule would be developed every 6 months that would enable employees to be prepared for the upcoming trainings that are within their Cohort of Small Groups for their Biannual training(s) as well as the additional non-essential sessions that they can attend.

We can't overload our employees so we must break the trainings up into chunks or small bites, so to speak, if we want them understand, remember and put into action what we are training them on. The Online sessions would be 1 hour with a facilitator that will know their cohort of employees they are working with so they can utilize the proper pedagogy and adult learning theory to train the employees effectively. There would be 4-8-minute chunks and then an 2-8-minute team activities and then 2-5-minute individual activities which would occur after each of the 8-minute chunks of information. The team activities would be completed through Kahoot or Quizlet or something similar. We would also do fun activities during the chunks including polls or sharing information utilizing Poll Everywhere, Popplet or Padlet. Trainers will not utilize PowerPoint they will use something different and fun such as Sway, Spark or Nearpod to enhance the training to the employees.

The topics will vary, as we remember the BYOD and the Security Culture are living documents and need to be adapted as technologies and the workplace advance and will change frequently requiring new training schedules biannually. But some of the more important training topics will be on:

- Different forms of cybersecurity including Social Engineering attacks, Malware, etc.
- Why they "employees" are important to the defense of SilverCorp's systems
- Importance of password security
- How to identify and report cybersecurity threats i.e. Incident Reporting
- BYOD Policies and Procedures

- Audit procedures and checklist
- Data Privacy Practices
- Insider Threats
- Safe Internet Habits
- Safe use of Social Media
- SilverCorp's Security Culture

We want to make our Security Culture effective and valuable to our employees so we want them to be involved in the growth of that culture and in order to do that we would also offer different sessions monthly to help them understand the Culture, why it is in place, why we have the Ambassador program and its purpose while also giving them the opportunity to share their experiences and to provide input about the BYOD, the Security Culture, the audits, etc.

The effectiveness of our trainings and other activities would be measured by auditing our employees, attaining the goals we set for SilverCorp and the participation in the non-essential sessions that are held along with surveys that would be completed quarterly on how the sessions and trainings are running. The surveys would include two multiple choice questions along with three open ended questions to help guide the training teams to greater success along with the Security and IT teams on how things are running with the BYOD program.

The critical piece our trainings and other sessions would be the participation of all employees including the C-Level which would also be apart of biannual training cohorts. SilverCorp employees need to understand and know that we are in support of the Security Culture and what to show that we practice what we preach. "Everyone in SilverCorp needs to be aware of the policies and the risks. They also need the right attitude because right attitudes create right actions. If your organization makes a deliberate and ongoing effort to improve your security culture, the benefits will be felt everywhere." https://cybersecurity.att.com/blogs/security-essentials/security-culture

Resources utilized but not referenced:
https://www.m-files.com/blog/top-7-risks-involved-bring-device-byod/
https://socpub.com/articles/the-biggest-byod-security-threats-and-how-to-avoid-them-9265
https://www.bizjournals.com/bizjournals/how-to/technology/2020/03/are-remote-workers-a-security-risk-to-your.html
https://cybersecurity.att.com/blogs/security-essentials/security-culture
https://www.mediapro.com/security-awareness-training/