Leslie Kahler
Cybersecurity Bootcamp
Homework Week 2

Assessing Security Culture

Step 1:
#1. Some potential risks of allowing employees to access work information on their personal devices include:

1. Lost or stolen devices: If a personal device containing company information is lost or stolen, then any company data on that device is also at risk of being compromised.
2. Unsecure networks: Employees accessing company information on unsecure networks, such as free airport WiFi or internet at a coffee shop, put company data at risk. According to CCB, "40 percent of mobile devices used for work get exposed to an attack in the first four months of use" (CCB Technologies and Bernhardt).
3. Malicious apps: When employees use personal devices for work, they could inadvertently download malicious apps or files onto their devices, making company data vulnerable to cyber-attacks.
4. Unsecure data transfers: When employees share files on their personal devices, they frequently transmit data without encryption. Without protections, all of the data on your mobile could be intercepted.
5. BYOD policy is not followed: having a BYOD policy in place can help with some of the above issues, but only if employees follow it. Employees using company devices on the company intranet pose less risk than employees using their own devices and hoping they follow the BYOD policy.

#2. While many security and IT professionals may prefer that employees only use company devices on the secure company intranet, this is simply not a practical solution. I believe the preferred behavior is that employees adhere to a BYOD policy that includes MDM software installation.
#3. While there is no real way to know how often your employees are using personal devices for work-related activities, the best way to get an idea of what percentage you're looking at is to send out an anonymous survey. If the survey is anonymous, you're more likely to get an honest response from employees.
#4. I think the goal will not be to establish a percentage of employees who do not engage in a specific behavior, but rather to train and incentivize employees to follow the BYOD policy, thus increasing employee happiness, employee productivity, and business profits (nibusinessinfo.co.uk).

Step 2:
In order to craft an effective BYOD policy for both the company and the employees, the CEO, CISO, CFO, Application Security, and HR need to be involved. The CEO needs to be brought into the conversation to give approval for any plans that are made. They will also help

communicate the changes made to the board. The CISO needs to be involved in any conversations involving information and data security and how to protect it. Making a BYOD policy will need to have input from the CISO to help determine what information must be protected and how to best go about protecting that information. The CFO should be involved because part of the BYOD plan will include making decisions about implementing these changes without impacting company profitability. Application Security needs to be involved in these conversations to determine how MDM software will be installed and managed. The last department that I believe needs to be involved in these conversations is HR. Creating a BYOD will include training sessions for staff so that they can understand the changes that have been made and the new policies that are in place.

Step 3:
A new BYOD policy will take several weeks to create, considering the meetings that will need to be held involving the different parties. Once the BYOD policy is created, a meeting with HR to discuss setting up training can begin. Because this new policy needs to be implemented for all employees simultaneously, training needs to be completed quickly. Assuming SilverCorp employs around 500 people, it should be possible to complete training in 2 weeks, with 20 employees engaged in a 1-hour training session that is offered three times each day. Ideally, training would be conducted in person so that employees can be engaged in the process, schedule a time to have MDM software installed, and sign paperwork at the conclusion of the session, rather than just turning on a training session and then completing other work while the training session runs in the background. Limiting each training session to one 1-hour should hopefully help with employee retention of information. According to Simplify Training, training sessions should include numbered handouts with bullet points that give only the most essential information. PowerPoint presentations should also use simple bullet points and be kept to 20-30 slides (Simplify Training). Adhering to these guidelines should help training be effective and meaningful for employees.

The training sessions should cover all of the BYOD policy information and why adhering to these policies is essential. According to Will Kelly with Tech Republic, training should be broken into ten sections; however, I believe the training sessions can be broken down into five sections. 1. Defining what BYOD means in the context of the organization: Training should begin with an introduction to why these policies and this training session are necessary. The key to any BYOD policy is getting employees to buy in. BYOD policies can create a 58% boost in productivity and 55% cost savings for employers, but lost or stolen devices caused 40% of large data breaches, and 50% of companies that allow BYOD have been breached via employee-owned devices (Brook). Getting employees to see the benefits of using personal devices but with restrictions will be a significant part of making these policies successful. 2. Cover the process of onboarding a device: Employees who want to use personal devices for work will need to be prepared that some company software will need to be installed on their personal computers. “Onboarding devices into a BYOD program can be done in conjunction with BYOD training. Even if you choose to onboard devices at another time, users need to know exactly what software their organization is installing on their personal device(s).” (Kelly). 3. Explain related expenses: Training sessions should cover company reimbursements for expenses related to using a

personal device for company business. “I put expense reimbursements high up on the training list because corporate usage of personal mobile devices means reimbursement for…data usage that a user with a BYOD device might incur. While service management and expense reporting policies should be clearly documented, BYOD training is the time to open up the discussion about the expense policies” (Kelly). This is the point where employees will want to know, “will the company reimburse employees a standard use fee, pay for certain applications or a portion of monthly bills?” (Brook). 4. Define the security policies: This portion of the training session should cover the use of corporate WiFi and the policies regarding the use of airport/hotel WiF as well as password policies. “For sensitive information, either belonging to the company or its customers, password protections are non-negotiable” (Brook). As employees use BYOD policies to work from coffee shops or airports, they need to understand if they need a dedicated hotspot or if they can use the free WiFi. Additionally, many employees may want to turn off lock screens on their phones or use weak passwords; how the company policy may necessitate a need for employees to change their habits needs to be clearly conveyed. 5. Review data ownership policies: BYOD training should also cover what data is considered proprietary or the property of SilverCorp and what data belongs to employees. This should include corporate vs. private email, social media usage, personal vs. corporate contacts, and what happens to that data if a device is lost or stolen or if the employee leaves the company. Employees will want to know if the company has access to their personal data and photos and what data they should expect to lose access to if they leave the company. 6. Teach about technical support and escalation practices: The last part of the training session should cover what technical support looks like for BYOD devices, what apps and programs are covered, and what employees should do in the event of a lost or stolen device.

After training is completed, we can gauge the effectiveness by consulting with IT and monitoring where any breaches are occurring and if they can be linked back to use or personal devices. Additionally, success can be measured by asking for employee feedback. Asking employees to complete anonymous surveys every six months where they are asked to honestly answer questions about their own BYOD use and their honest thoughts on the policies in place. Ultimately, BOYD policies have been linked to increased employee productivity, cost savings for the company, and ease the ability to work while traveling or work from home, but it only works if it is followed, and employees are most likely to follow them if they understand why they are in place and that the benefits out-weight any restrictions imposed through these policies.

Bonus:

1. Blacklisting: One preventative, technical solution could involve blacklisting non-approved sites from employee phones. Programs that could be blacklisted could include games, and social media and dating apps, in addition to filing sharing apps. Blocking file-sharing apps could be particularly important. According to Brooks, “file-sharing services are another category of apps that often find themselves on blacklists, as companies fear that sensitive information could be shared with unauthorized third parties, either intentionally or inadvertently, by employees” (Brook). The flip side to blacklisting could be whitelisting, where, rather than blocking non-approved sites and apps, only a list of approved sites and applications are approved. The advantage to both whitelisting and blacklisting is that

they can help promote employee productivity and data safety by keeping them off non-approved sites; however, both are pretty restrictive and can hinder employees outside of work. Employees should be able to play games on personal devices outside of work, and this technical solution does not allow for that possibility.

2. Encrypting Data: This is a simple, preventative technical control. We should always assume that a breach is inevitable. By encrypting sensitive data, we can help to mitigate risks from employees sharing data over unsecured networks. One advantage to this solution is that encrypting data is also beneficial outside of BYODs - it can also help protect data from a breach that occurs outside of employee use of personal devices. A downside is that encrypting data is that it can lead to a false sense of security. "A disadvantage of encrypted files is that relying on them to keep things secret could lull you into a false sense of security. A determined person may marshal overwhelming computer resources to decrypt your secret files" (Vandersteen).

Bibliography

Brook, Chris. "The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits." *Digital Guardian*, 24 November 2020, https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating. Accessed 1 April 2021.

CCB Technologies, and Melody Bernhardt. "BYOD: How your business can address the 5 biggest vulnerabilities." *CCB Technologies*, https://ccbtechnology.com/byod-5-biggest-security-risks/. Accessed 30 March 2021.

Kelly, Will. "10 essential elements of BYOD training." *Tech Republic*, 21 February 2013, https://www.techrepublic.com/blog/10-things/10-essential-elements-of-byod-training/. Accessed 1 April 2021.

MXO Tech. "5 Tips for implementing a secure BYOD policy." *Mxo Tech*, 6 June 2018, https://www.mxotech.com/2018/06/5-tips-implementing-secure-byod-policy/. Accessed 1 April 2021.

nibusinessinfo.co.uk. “Bring Your Own Device: benefits and risks.” *nibusinessinfo.co.uk*, https://www.nibusinessinfo.co.uk/content/bring-your-own-device-benefits-and-risks. Accessed 30 March 2021.

Simplify Training. “How to Conduct an Effective Training Session.” *Simplify Training*, https://simplifytraining.com/article/how-to-conduct-an-effective-training-session/. Accessed 1 April 2021.

Vandersteen, Julius. “The Disadvantages of Encrypted Files.” *It Still Works*, https://itstillworks.com/disadvantages-encrypted-files-2597.html. Accessed 1 April 2021.