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.

With a first Google search, I have stumbled upon an excellent article on m-files.com regarding potential security risks involved with BYOD (Bring Your Own Device).

As mentioned in the article, advances in technology and perceived costs of providing company owned secured devices made using personal devices a very affordable option for employers. In that way, employees had to keep track of only one device, which gives convenience of managing work and personal items in one place.

The article mentioned the “2019 Intelligent Information Management Benchmark Report” in which survey respondents indicated that over 60% of employees use basic commercial grade file-sharing apps and/or personal devices to access and share company information, but more than half of companies (52%) discourage or prohibit the use of personal devices.

In this homework assignment, I will be presenting a possible solution for a fictional company called SilverCorp.

According to the m-files.com article, the of the top BYOD risks are:
-Using an unsecured Wi-Fi network, which leaves the device open to attacks such as the man-in-the-middle attack.
-Malware Infiltration which can happen, for example, when the user downloads a game with hidden malware
-Phishing (clicking on unfamiliar links/attachments received in email could lead to data leak)

2. Based on the above 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.

Preferred employee behavior when using personal devices would be:

1. If possible, use company provided secure devices to access company data.
2. Dedicate only one device for accessing company data.
3. Make sure to always have the latest OS updates and security patches installed.
4. Make sure to have an antivirus/anti malware and firewall software with the latest updates installed on the device.
5. Not to download any company data onto the said device.
6. Avoid downloading files/games from untrusted sources.

7. Avoid clicking on unfamiliar links received in email, and only trust email received from a verified source.
8. Avoid using public networks.
9. Not using rooted/jailbroken devices.

3. 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.

1. Regularly sending a test link from a freshly made email account to see how many employees click on it, disregard the validity of sender/content and unintentionally leak data. This could be done by sending a link leading to a simple online document requiring employees to type their name and confirm that they've read it.
2. Keep IP logs of devices accessing the company data to see how many devices employees use to access the data and from where.
3. Conducting a survey to see what type of devices do employees use to access company data and if any of those devices are rooted/jailbroken.

4. 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.

The main goal would be for all of the employees (at least 95%) to adhere to company security guidelines to avoid unwanted data leak/cyberattacks.

Step 2: Involve the Right People

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

- Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.

CEO - Must understand the risks and assume responsibility for the organization’s cyber security. Work closely with CISO to establish a cybersecurity strategy for specific cyber risks that the company has. Make sure that all of the employees are trained and up to date with any new security threats.

CISO - Responsible for cybersecurity. Analyzing all possible threats for the company and mitigating risks. Working closely with the IT department on creating a secure interface for employees to use when accessing company data from personal devices. Making sure all possible cyber vulnerabilities in the company are covered.

CSO - Laying down the new security rules and guidelines. Creating training materials for employees using personal devices to access company data. Testing and measuring the effectiveness of the new rules, regulations and guidelines.

HRO - Providing guidance and training on every aspect of company policies and procedures. Makes sure the employees are regularly reminded of the guidelines for personal devices. Taking notes of any problems employees might have regarding the new rules and guidelines.

IT - The IT department works closely with the CISO to help strengthen the company’s cyber security. Offering to inspect, scan and update software on employees’ personal devices to make sure the devices are safe to use for accessing the company's servers. Making sure all of the company’s computers and other devices are running up to spec and up to date with latest updates and security patches.

Step 3: Training Plan

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

The training would be a compulsory event held every 6-12 months via a seminar that could be followed online should the employee be unable to attend in person.

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

Topics covered would be:
-The importance of security when using a personal device to access company data.
Employees need to be aware that the devices they use are always at risk of a cyberattack.

-Most common cybersecurity threats that plague the world and are immediate danger to the company
They also need to know which cyber attacks are most commonly used at the current time and how it can affect them/their devices.

-Measures to protect and secure the personal device against such threats
A refresher lesson on internet security to avoid falling for most common threats such as phishing.

-Maintaining the security of both the personal device and the company devices
A reminder to frequently check for security updates for their devices and the software used on said devices.

-New rules/guidelines (if any)
Employees will be reminded of any new rules and guidelines that have been issued or will be issued in the near future.

-Future plans to further improve cyber security within the company.
A brief overview of plans for the future of company's security in the cyber world.

3. **After you've run your training, how will you measure its effectiveness?**

-As mentioned previously, a good practice would be a regular (every 1-2 months) test by creating a new email account and sending a test link/attachment to employees to test if they are checking the validity of the sender/email.

-Conducting regular (every 3-4 months) surveys where employees would anonymously express their satisfaction with the new rules/guidelines and to write down anything that could be changed/improved to improve employee comfort and satisfaction.

-1:1 Discussions with employees every 6-12 months to assess their knowledge of the rules/guidelines, discussing what they do to stay secure and giving tips to help them further be secure when using a personal device for accessing the company's servers.

Bonus: Other Solutions

- Indicate 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?**

Considering the measures implemented so far, I believe that 95% compliance is achieved and the risk of data leak or cyberattack mitigated. But what do we do with the other 5%?

In that case I would be working on putting in more rigorous measures to make sure the rules and guidelines are followed, such as:

-With the measurements already implemented we would be able to see which employees are continuously not following the guidelines and such behaviour is not in the company's best interest. The solution would be a written, then verbal warning which could ultimately lead to termination if the employee behaviour doesn't improve

TYPE: Administrative
GOAL: Preventative - Improvement of employee behaviour to respect and follow guidelines to minimise any risk of data leak/any kind of cyberattack.
ADVANTAGE: Strengthened company's cyber security
DISADVANTAGE: Employee satisfaction may be negatively impacted.

-If the above method still proves to not be enough, the company might have to ultimately go for a costly solution which would affect all employees but would assure the security and safety of the company's assets.

That includes creating an app that every employee who uses their personal device to access company data must install on their device. It would serve as an interface to connect to the company's servers with continuous logging of employees accessing the data and continuous logging of device usage. The app would monitor what the employee is using the device for (which apps are they using, browser tracking with cross referencing with known malicious sites) to, if a malicious activity is detected, revoke the access to company data until the device is secure and employee warned/trained.

TYPE: Technical/Administrative
GOAL: Detective/Preventative - Maximum security of data servers.
ADVANTAGE: Minimised risk of data breach/cyber attacks
DISADVANTAGE: High cost of creating and implementing such app.

Finally, I believe that the second of these two bonus solutions would not be necessary since the first one might be enough to correct employee behaviour and SilverCorp will be able to continue doing business securely.