General
    Note on the Bonus Section
    Terms

Step 1: Measure and Set Goals
    Question 1
        Security Risks
        Potential Attacks
    Question 2
    Question 3
    Question 4

Step 2: Involve the Right People

Step 3: Training Plan
    Frequency
    Topics Covered
    Measuring Efficacy
        Lowered Breach/Incident Numbers
        Remote Device Wipe Numbers
        BYOD Usage Decrease

Sources Used

General

Note on the Bonus Section

I didn't include a bonus section in this document. However, I did incorporate a couple non-training related solutions to BYOD usage in the policy discussion.

Terms

BYOD → stands for "bring your own device"; I'll use this as shorthand at times for an employee's personal device.
IT → I use this as a generic term for network administration, system administration, security departments, etc.

Step 1: Measure and Set Goals

Question 1

Security Risks

There are numerous security risks to employees using their own data. I'll try to focus on the tech risks.

- Data Theft

    - Employees using their own devices inevitably means company data will get stored on their devices. Company data existing on an uncontrolled device puts that data at higher risk for theft.
- Malware
    - Since the company doesn't have nearly the control over an employee device, employees can more easily install potentially harmful software.
- Unsecure Network
    - Unless the company uses a VPN for all work related web traffic, the employee device will undoubtedly sit on average a weakly secure network.
- Difficult Device Management
    - In the event an employee leaves an organization, sensitive data and/or username and passwords could still be on the employee's device. Securing that information could be tricky at best and impossible at worst.
- Ineffective Compliance Enforcement
    - If and when the company does have a security policy, trying to enforce that policy on an employee's device can present some challenges. Enforcing the policy could inadvertently violate an employee's privacy.

Potential Attacks

- Device Theft
    - Given the device belongs to the employee, the device will no doubt leave the office -- an inherently more secure physical environment. Attackers looking to intentionally target the company could through research discover that the company allows BYODs and attack these devices instead of the company network infrastructure.
- Malware
    - As mentioned above, a company's network can lock down a lot of potentially harmful websites and random "updates". However, an employee is most likely not that savvy. Malware could infect a BYOD which then could propagate to the company network. Or Malware could simply relay information about the company to an attacker if and when the employee accesses the company network.
- Password Cracking
    - A company can institute password strength requirements on their devices. However, a company cannot enforce that on an employee's device without some other policy/software in place. And BYODs will in most cases have weak passwords. An attacker that cracks a BYOD's password could then use that device to gain access to the company network.
- Windows and RDP (Honorable Mention)
    - Inexperienced computer users can often leave port 3389 open on their computers -- port 3389 is the port most commonly associated with RDP. Windows RDP has a long history of exploited vulnerabilities.

Question 2

Given the implication there's no policy or safeguards in place for BYODs, I would expect no employees to use their own devices. However, that would present significant challenges for the company. We would need to provide devices for 25% of our employees which could represent a significant financial burden. Also, this could lead to a drop in productivity as employees adapt to using new devices and adapt to only working in the office.

Given the challenges of forbidding BYODs, the following behaviors are preferred if an employee uses their own device:

- Install a device policy app allowing system admins to enforce password requirements and remotely wipe devices in the event of theft, loss, or termination of employment
- Connect to the company network and company applications through a VPN
- In general, learn security-focused habits and skills

Question 3

The network administration team could easily monitor network traffic to determine BYOD IPs connecting to the network. Assuming the company's applications are capable, the system administration team could monitor for BYOD machines that connect.

Question 4

These are closely related to the efficacy measures enumerated below.

- Catch all incidents of BYOD theft, loss, and termination of employment and wipe the devices
- All BYODs that connect to the company network connect over a VPN
- See a small to medium drop in BYOD usage as employees who don't wish to adopt secure BYOD practices stop using them

Step 2: Involve the Right People

- CEO
    - Since this policy change will affect the entire company, all teams we'll need CEO buy-in. Also, the CEO will perform the initial communication of the policy to the company as a whole in either a convention or mass online presentation.
- CISO
    - This person will work closely with his teams and come up with the initial plan and budget proposal for the policy system. They will most likely communicate and present to the CEO.
- Network Security
    - Network Director
        - This person will develop a plan to target BYODs for special monitoring.
    - Network Administrator
        - This person will implement the plan set forth by the Director. They will undoubtedly need to enforce future security measures to limit certain BYOD network traffic.
- System Administration
    - This person will need to enforce a new password strength plan on all devices including BYOD devices. They will enforce this using device security policy apps. They will also wipe devices remotely in the event of theft, loss, or compromise.
- Incident Response
    - Incident Handler
        - This person will investigate and report on incidents that occurred on a BYOD. While they have no doubt dealt with BYOD issues in the past, they'll take part in more detailed individual incident reporting as well as a top down look at BYOD incidents as a whole.

Step 3: Training Plan

Frequency

For new hires, the training should definitely take place in person during new employee orientation and/or training. This will lay the best foundation for instilling good security habits for all new employees.

For current employees, the following formats should help set the foundation for instilling a security culture: in-person seminar and online videos to cover specific topics in more detail. These formats will only happen on the initial rollout of the campaign.

Going forward, a mandatory online refresher covering new security topics or any potential changes should occur once every three months.

Topics Covered

- Overview of potential attacks and vulnerabilities
    - This introduction will hopefully get people to start thinking about device usage in general through a security-focused lens.
- In-depth coverage of vulnerabilities and attacks that affect BYODs specifically
    - This will educate employees further and hopefully help them make better decisions about
- Use of the company VPN for any device connecting directly to the office network
    - This will encrypt data sent to and from the employee device and the company network
- Mandatory use of a security policy app for mobile devices
    - Example: Google Device Apps Policy
    - This will effectively make employees register their mobile devices with IT
    - Enforce a password strength and expiration policy
    - This will allow IT to remotely wipe the device in the event of theft or tampering

Measuring Efficacy

Lowered Breach/Incident Numbers

Without any policy before this regarding BYODs, the company has no doubt experienced a relatively large amount of breaches and /or incidents originating from BYODs. Ideally the company's security teams have tracked that data. And more ideally, the policy would lead to a significant reduction in those breaches and/or incidents.

Remote Device Wipe Numbers

Any remote device wipe numbers would tell us that the policy is succeeding. The company had no data on those numbers in the past. Any data going forward would lead us to believe incidents of theft or loss are now getting addressed.

BYOD Usage Decrease

A decrease in the number of employees using BYODs would also indicate policy success. Some employees might not want the extra hassle to use their own devices.

Sources Used

- https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember
- https://ccbtechnology.com/byod-5-biggest-security-risks/
- https://www.itproportal.com/2015/07/13/the-good-bad-and-who-knows-about-byod/
- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=rdp+windows
- The three slide presentations for this unit of the course