1. There is an array of security risks that bring-your-own-devices (BYOD) bring to the workplace. Network compromise due to malicious app downloads, data loss and/or network compromise because of device loss or poor device password security, and credential and information compromise from a man-in-the-middle attack from unsecured network usage are just a few of the risks.

For example, a program from an unapproved app store could be just a trojan masquerading as a real app, which could then be downloaded onto the user’s device. There are many forms of trojans, but the worst are remote access trojans, which allow remote access to the entire device and would compromise the company network that it is also remotely connected to.

If a phone or tablet is lost or stolen and the information on it is accessed, then any information from work that is stored on it should be considered compromised. The situation is made worse if the device is not password protected or the information on it is not encrypted. The phone should be able to have its memory wiped clean to mitigate the risk of the information being used maliciously.

A man-in-the-middle attack is much more apt to happen on an unsecured public

network without the use of a VPN than on a secure network connection. However, many people use their devices at public hotspots and leave themselves open to vulnerabilities. A man-in-the-middle attack intercepts network traffic and can eavesdrop on information that is sent and received giving access to data, user credentials, and possibly confidential company information.

2. There are various ways to prevent these types of attacks from happening. Since over

75 percent of employees are doing work related activities on their personal devices it

makes sense to choose a security program that is quick and easy to implement for both the employees and the company. Allowing employees to opt-in to a mobile device management software (MDM) for the use of their personal devices for work purposes is a fantastic way for IT to maintain security on all mobile devices. It allows them to regularly install security updates, install specific software use for work and create app segregation and VPN for the user. IT can remotely wipe the device if it is stolen or lost and will also have control of revocation of access and removal of company files and information if an employee is terminated or leaves the company.

3. In order for the employee to use their own device off-campus or remotely log-on to the

company network, they would need to have the MDM software installed on their device

and sign a company user agreement. Software such as Soti MobiControl, or Mobile Iron

exist for this purpose and are highly successful in making sure users have secure access to the company network on a personal device. With one of these types of programs it will ensure that all endpoint access is secure for all mobile devices.

All employees would also have to participate in an employee cyber security awareness program to ensure a well-rounded understanding of cyber security issues such as phishing, shoulder surfing, social engineering, tailgating, and other ways criminals gain information or access to information from employees. Several whole system training programs are available for purchase and offer a variety of services at different price points. No matter what the program, the key to successful employee training is for the program to be clear, training to occur at regular intervals, training to be relevant and most of all to be interactive. The cyber security awareness program is applicable to all employees not just those who want to use their own devices to use at work. Such programs include, KnowB4, Proofpoint, Mimecast, Sophos, and Cofense, although there are many more to choose from.

4. The goal is to have all employees that remotely access the company servers

from personal devices use the MDM software, thus ensuring that company policy is

followed and off-campus access is secure. If they do not opt-in to the program, they will

not be able to use their personal device for work purposes.

5. From the start, a base set of company needs and wants for the MDM program and the

employee cyber awareness training needs be acknowledged. First, the Director of network security needs to come up with a “wish-list” of sorts that he or she would prefer so that the highest security protocols can be met. He would select a preferred MDM program and cyber awareness that he or she wants to implement. The *Director of Network Security* is concerned with making sure that the network is secure and that the protocols of network policies as set forth by the company are carried out. Second, the *Chief Information Officer*, usually the head of IT, would need to approve the wish-list. He is concerned with making sure company security policies are carried out by the IT department. Third, the *Chief Information Security Officer* would need to make sure that the proposal sent from IT mitigates the risks that the company foresees in the future. The Chief InfoSec Officer makes risk assessments and ensures that assets are adequately protected. He would need to assess whether the MDM and cyber awareness programs meet or exceed the needs of the company and whether or not the programs would mitigate the risks that the company faces. Fourth, the *Chief Financial Officer* would have to make sure that the MDM and cyber awareness programs that are chosen not only meet the needs of the company but also make financial sense for the business as a whole. The Chief Financial Officer will have to weigh the amount of money that could be lost to the company if a breach would occur in relation to the amount that the programs cost annually.

**Training plan:**

1. **Onboarding**

When an employee is first hired, he or she must be trained on the overall expectations of the company security wide. This is also true with mobile device usage; they can opt-in to use the MDM program on their own home device. It needs to be made clear to them that to connect securely to the company remotely that they *must opt-in or their device will not be able to access business servers.* They will need to temporarily physically hand the device over to IT for them to complete the process and sign a company policy agreement about using company software remotely and in a responsible manner.

As one of the first steps in the hiring process, a new employee also needs to create an account with the cyber security awareness program that was chosen and c*omplete the first training segment before**continuing with complete company network or server access.*

Cyber security awareness programs and other whole system training programs have *online intermittent training.* They also occasionally send out fake phishing emails to see if employees will click on them to measure how well each employee is learning and to keep them aware. Employees that continue to click on phishing emails must complete remediation training and will be sent emails telling them to do so.

1. **In-person annually**

In person training should occur at least *annually*. Topics that will be covered in in-person

training will be physical in nature. Themes such as social engineering and shoulder

surfing will be touched upon, since this is not something that can be easily learned

online.

Within social engineering, there are a variety of subtopics that will be included such as

* Baiting
* Pretexting
* Quid pro quo
* Tailgating

There are also social engaging engineering conferences that are offered around the nation in accommodating locations such as the annual *Human Hacking Conference* (this year in Lake Buena Vista, FL) that employees would be encouraged to attend.

1. **Post-incident**

Anytime there has been an incident or breach, it presents an opportunity for *refresher training*. Not only will there be an investigation into the incident and how and when it occurred but into the events leading up to it and what allowed it to happen. After each incident, the overall security plan needs to be reviewed and updated to make sure it takes into account changing circumstances, technological advances, and future security expectations.

**Conclusion:**

There are multiple security concerns mitigated with using a Mobile Device Management  
 (MDM) program for bring-your-own-devices (BYOD) for work use. Although the user is

essentially giving up some privacy of their personal device, they are making a

decision of whether they are willing to do so for convenience and for the

security of the company. This is a technical control that is implemented by IT, but

because access rights can be revoked and the user can be shut out of the system for

whatever security reason, administration also has a hand in the decision making

process.

MDM programming creates app segregation through mobile application

management (MAM) essentially sandboxing and controlling the apps needed for work

and keeping it separate from personal apps and other information on the user’s device.

This decreases the likelihood of malware from making its way from downloaded apps or websites on the user side of the device into the workplace environment. Also, by creating a VPN or Virtual Private Network for the user to connect to, it creates a secure way to remotely connect to the company server. *However, as 75% of the company is using bring-your-own-devices for work use, the risk is highly likely that incidents will occur on a regular basis and that a breach is imminent.*

The advantage to implementing the Mobile Device Management solution is that it

resolves many security risks in one cohesive design. It is relatively easy to implement,

although it will take time to be uniformly applied to all company devices. It would make sense to roll out installs in multiple phases depending on device type and user access credentials. The disadvantage of using an MDM solution is that the company employees may not want to give up the sort of control of their devices and privacy that is necessary for the installation of this system. *Mobile Device Management allows the company to take company security policies and apply them uniformly across multiple devices and platforms and allows IT professionals to better detect unauthorized access.*

The use of online cyber awareness training programs is widely used by large and small businesses and they are finding that the amount of phishing email incidents decrease significantly with regular use and training. They are fast and easy to implement, although not necessarily inexpensive. *In this case, over 50% of the company employees are checking their work email on BYOD devices and this poses a significant risk not only to data loss, but also to compliance, confidentiality, and legal liability.*

In addition to online cyber awareness, in person workshops that integrate topics of

physical cyber security compliance issues and best security practices are a necessity.

They do not have to be elaborate, but can be included in a company picnic, or other

event that makes the training engaging for all those involved.

The inclusion of a Mobile Device Management program, an online cyber awareness

training program and an annual in-person training session provides a well-rounded

program that tackles the problem of employee-based cyber security needs from multiple

facets. *Together they will significantly decrease the cyber security risks associated with work performed on employee owned devices as well as those risks associated with employee error.*

Sources:

<https://privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk>

[https:/](https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate)<https://sourceforge.net/software/mobile-device-management/free-version/>

[/www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate](https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate)

<https://www.pcmag.com/picks/the-best-mobile-device-management-mdm-solutions>

<https://www.threatstack.com/blog/how-to-implement-a-security-awareness-program-at-your-organization>

<https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/knowbe4/alternatives>

<https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html>

<https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html#:~:text=9%20types%20of%20malware%20and%20how%20to%20recognize,and%20exotic%20forms.%205%205.%20Ransomware.%20More%20items>

<https://www.secsign.com/business/two-factor-authentication/>

<https://searchmobilecomputing.techtarget.com/feature/Pros-and-cons-of-using-secure-containers-for-mobile-device-security>