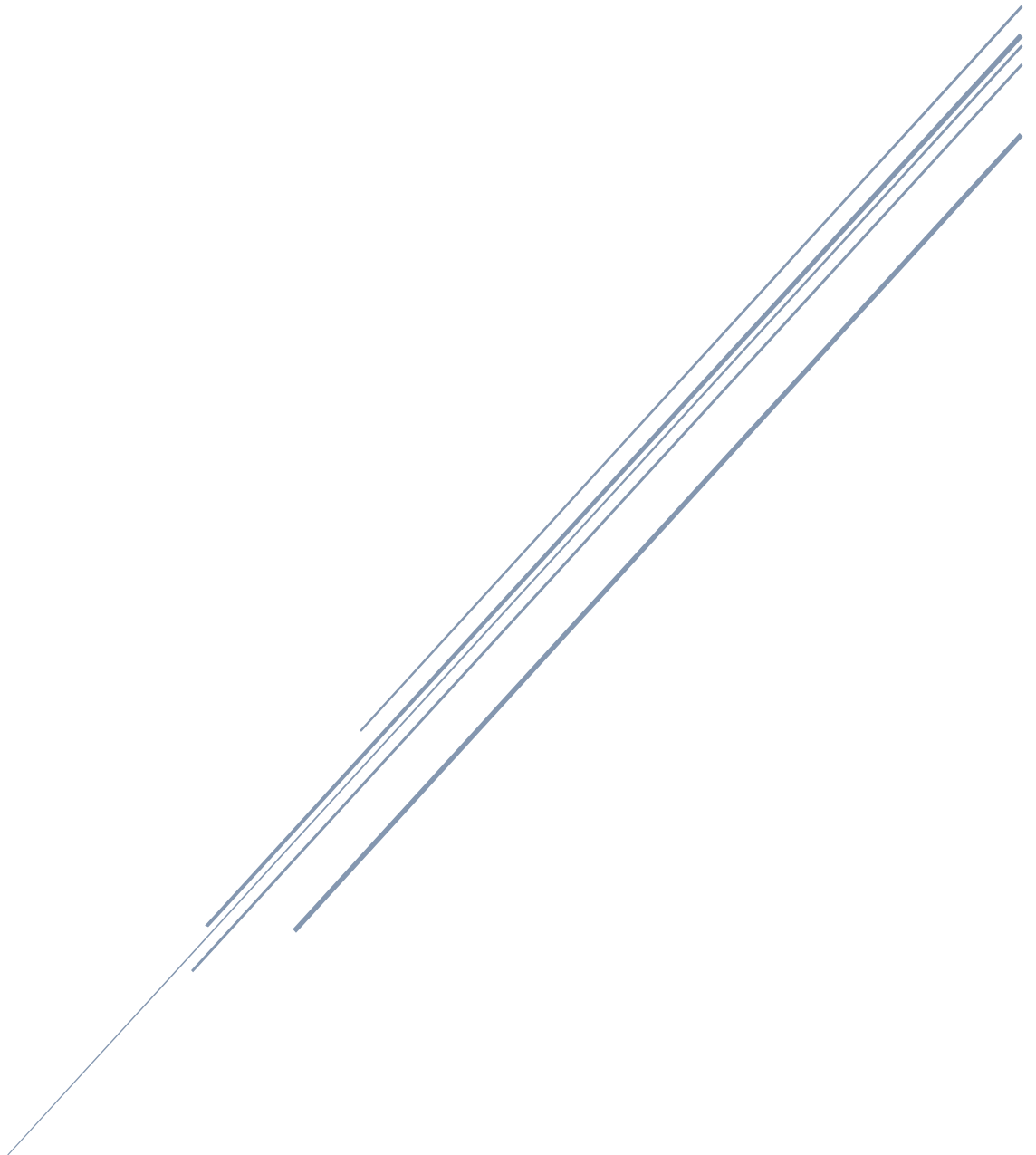


INFORMATION TECHNOLOGY AND SECURITY

Bradley Martin

MAR16829326

08/05/2019



Assignment 2
HND Applied Computing

Contents

Introduction	2
Research.....	2
What is BYOD	2
Advantages of BYOD	2
Disadvantages of BYOD.....	2
What is MDM	3
Advantages of MDM	3
Disadvantages of MDM.....	3
Implementation	3
Mobile Device Management Chosen.....	3
Flowchart	4
Cisco	5
User Policy.....	7
Email Policy	7
Password Policy.....	7
BYOD Policy	7
Backup Policy	7
Findings & Conclusion.....	7
Bibliography	8

Introduction

Hyper Fort have given me the task to evaluate BYOD and implement it into their network. This report will include information on BYOD and the advantages and disadvantages of using it. It will also contain information on MDM software and which one I believe is best in comparison of others to use. I will also be creating policies for the company.

Research

What is BYOD

BYOD stands for 'Bring Your Own Device'. BYOD is used in companies to allow employees to bring their own devices from their household to use at work. BYOD has both advantages and disadvantages that can be taken into consideration when a company decides if they are going to allow it within the workplace.

Advantages of BYOD

BYOD has multiple advantages for the company and also the workers such as improving the employees' satisfaction in the workplace, this is because the employees will be able to use devices that they are familiar with, due to this it could also improve the overall productivity within the company. [1] This also prevents the employees from having to use software that they are unfamiliar with, an example of this is people who use apple products instead of windows products. There is a chance that the employee may not like the equipment or software that is provided by the company so BYOD also prevents this issue. Another advantage of using BYOD is that it saves money within the company. This is because it saves having to buy devices for each individual employee because they are able to use their own. [2] Because employees are able to use their own devices they are able to easily work at home, this will allow the employee to work more flexibly and also potentially reduce stress levels for the employees. One more advantage is that employees will also take more care of their own personal devices, this is because they know that they will have to replace it themselves if something were to happen to it which can sometimes not be the case when companies provide the devices for the employees, this is because the employee is aware that the device will be replaced by the company if something were to happen to it.

Disadvantages of BYOD

BYOD also has multiple disadvantages with the first being the security. Security is probably the biggest issue with BYOD, company provided devices are much less likely to have data leaks compared to the employees' personal device. Personal devices also have personal data on them, this makes it harder to remove any data if an employee were to leave the company or lose the device, some MDM software are able to deal with this though. The company will also have to make sure that every device is secure itself and has appropriate protection from malware which may not be the case for personal devices. Another disadvantage is the costs for the employees, some employees may be not have the device and may be unable to afford a reliable device for their work and if something were to happen to the device after the amount of travelling the employee would do then it may cost even more for replacements. Another disadvantage for BYOD is that employees may use multiple personal devices and some companies lack the network infrastructure that is able to handle that amount of traffic that the devices will bring.

What is MDM

MDM stands for 'Mobile Device Management' and is software that is used within companies by the IT administrators to monitor an employees' personal devices such as smartphones and laptops. MDM would be used by companies to enforce policies that the company has put in place for these devices. [3]

Advantages of MDM

There are advantages to using MDM such as having the ability to setup automatic updates on user devices, this allows critical security patches to be easily applied on personal devices whenever necessary. Another advantage is that it is possible to manage the employees' work files without touching the employees' personal data. Some MDM software offers an automated device registration which allows an employee who owns a device to receive an email which allows them to register their device. [4]

Disadvantages of MDM

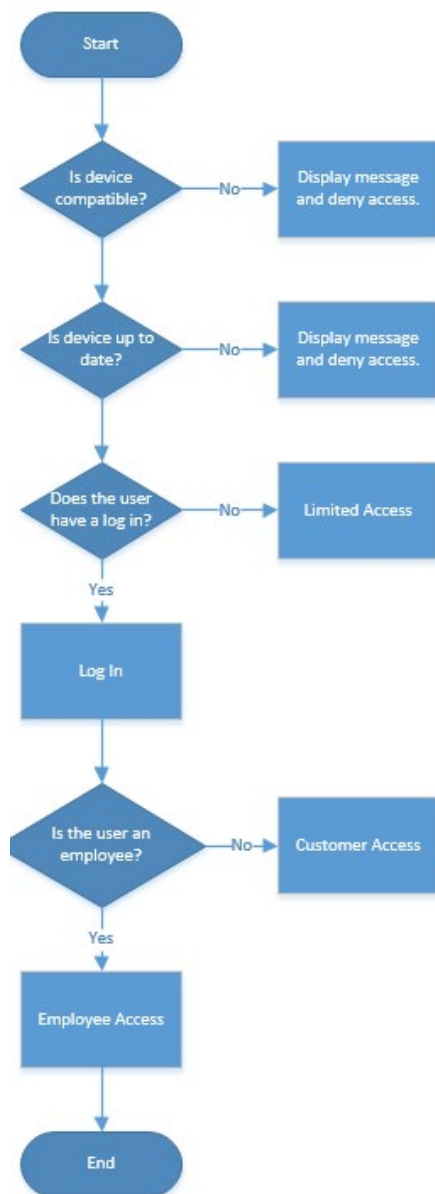
However there are also disadvantages to MDM such as the providers having a hard time providing support when new operating systems are released for devices. Another disadvantage to MDM is that employees are able to install third party applications and the company is unable to stop this due to them being personal devices, this affects the overall security within the company.

Implementation

Mobile Device Management Chosen

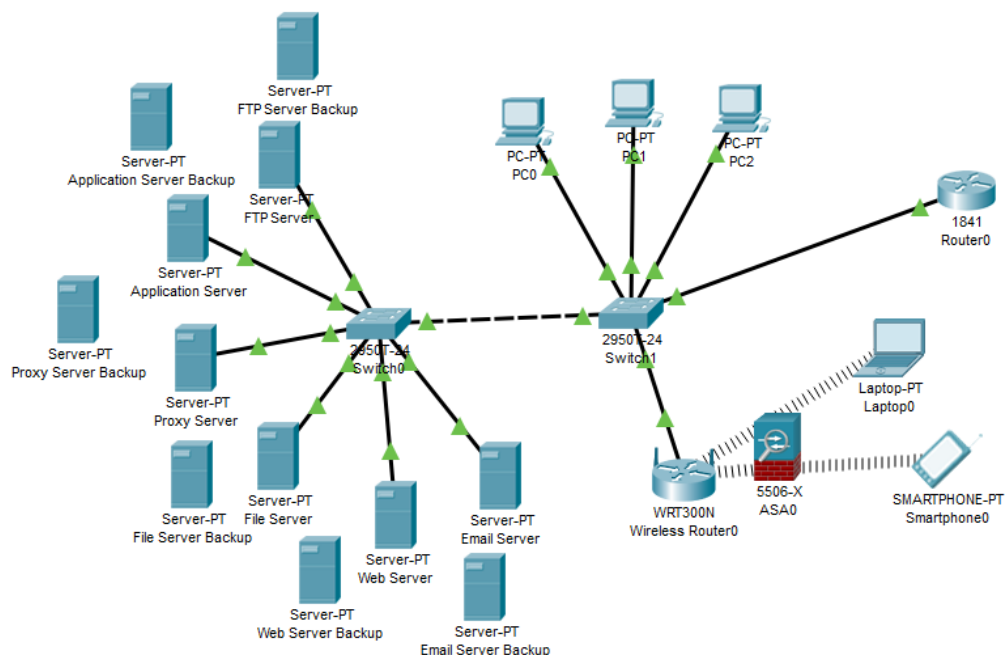
I have decided to use the software called VMWare Airwatch. This is because of what this MDM offers in comparison to some off the other MDM software that is currently available. VMWare Airwatch has a bunch of capabilities including functions that support BYOD. One capability is that it allows the company to enable employees to access applications from their own personal devices. This MDM also allows you to give users access to business applications through a single catalogue. VMWare Airwatch also has capabilities that enhance the security. This MDM provides a functionality known as enterprise wipe, this feature allows employees to automatically have their access revoked if they were to leave the company, lose their device or if they were to break any important policies [5]. This is a functionality that some MDM software isn't capable of such as Microsoft Intune and Amtel Telecom. VMWare offers extra functions such as mobile expense management also known as MEM. MEM is a function that allows data usage to be monitored and controlled to save money in the company expense. This is a feature that some MDM software aren't capable of such as Microsoft Intune and Citrix XenMobile [6]. Another feature that VMWare Airwatch offers over others which is known as geofencing, this feature is used to secure company data in devices that travel out of certain areas. Geofencing allows the company to create 'safe zones' that allow company data to be used completely while it can somewhat restrict the company data when it isn't inside a 'safe zone' these zones can be set to different sizes such as the size of a city.

Flowchart



This is the flowchart that I have created to demonstrate how the MDM could work when a device is connecting. It first checks if the device is compatible with the MDM that I have chosen and if it isn't compatible then it will display a message telling them that while denying access. It then checks if the device is up to date for security reasons and will also deny access to the device if it isn't up to date. It will then check if the user has a login which will help determine what access the user will have. If the user doesn't have a login then they will receive limited access but if they do then they'll be able to login. It then checks what type of access they should have, if they are a customer then they will be assigned with customer access while an employee gets the employee access.

Cisco



This is the network that I created on Cisco Packet Tracer. I've added security to the network by adding a firewall to prevent all wireless devices from connecting. This will make it so only authorised personal devices are able to get into the network. On the left side of the screenshot are the servers, there are six appropriate server that would be used on the network along with backup servers for each of them in case of hardware failure. The route in the top right will be used to enable DHCP. Next I added the wireless router, this would allow wireless devices to connect to the network. The ports that were inactive on the switches were turned off as they should be.

Authentication		WEP Key	
☐ Disabled	☐ WEP		
☐ WPA-PSK	☒ WPA2-PSK	PSK Pass Phrase	Password
☐ WPA	☐ WPA2		

To allow devices to connect wirelessly I set the authentication to WPA2-PSK and enabled a password that devices would need to have to connect to the network. This should allow personal devices and external connections to happen easily. I've also added a firewall add an extra layer of security to the network.

```
Router(config)#enable password byod
Router(config)#enable secret cool
Router(config)#line con 0
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
Router(config-line)#password byod
Router(config-line)#exit
Router(config)#
```

```
Switch(config)#enable password byod
Switch(config)#enable secret cool
Switch(config)#line con 0
Switch(config-line)#login
% Login disabled on line 0, until 'password' is set
Switch(config-line)#password byod
Switch(config-line)#exit
Switch(config)#
```

I added security to the network by adding passwords to the devices. Whenever someone wants to gain access to the console of them then they'd need to enter the password that I have set.

User Access Verification

Password: |

Switch>enable

Password: |

This shows up whenever you attempt to get into the console or router, this is an extra layer of security to prevent unauthorised access into the network devices. If the password is correct then another password will appear once the user tries to 'enable'.

User Policy

Email Policy

1. Emails shall not be used for the usage of creating disruptive or offensive emails.
2. Users must not use third-party email systems for Hyper Fort related business.
3. Work related emails must only be used for work related business and not personal.

Password Policy

1. Passwords must have a minimum of eight characters.
2. Passwords must be alphanumeric with at least one capital letter and special character.
3. Passwords are encouraged to be completely unique and not used for other devices or accounts.
4. Passwords must be changed at least once every three months.
5. Users must not re-use any of the last five previous passwords that they have used.
6. Passwords must not be shared with anyone, this includes co-workers and supervisors.
7. Passwords must not be written down or physically stored.
8. Users must not use the "Remember Password" ability that is available on software.

BYOD Policy

1. Hyper Fort will recommend software and specifications for personal devices as some devices aren't compatible.
2. Devices must be automatically locked if left idle for five minutes.
3. All Hyper Fort related data must be encrypted.
4. Personal devices must be password protected to prevent unauthorised access.
5. Lost/stolen devices must be reported to the Hyper Fort within 24 hours.
6. If a personal device is reported missing then all Hyper Fort related data will be removed from said device.
7. The user will have to make sure precautions are taken to ensure that all personal data.
8. Users are liable for all costs that are associated with their own personal device.

Backup Policy

1. Backups of data must be made regularly.
2. Logs must be created for backups, this will include the date of the backup and if it was successful.
3. All backup drives must be stored offsite.

Findings & Conclusion

After researching and creating this report I have learnt multiple things. The first being that I've learnt more about BYOD and now have a better understanding of it including the many advantages and disadvantages that come to using it in a company, I do however still think that BYOD is overall an advantage for the company and employees' working there. I've also learnt about MDM and how much it can help BYOD within a network, I've also learnt about the advantages that certain MDM software can provide along with some of the disadvantages. I have also learnt how to create a policy and some of the key things needed to be involved with the policy. I believe that in future work I can improve the amount of research that I do when creating reports, I feel this way because the research helped me completely when it came to understanding BYOD along with MDM.

Bibliography

- [1] "The Advantages & Disadvantages of BYOD," [Online]. Available: <https://www.1rti.com/the-advantages-disadvantages-of-byod/>. [Accessed 4 May 2019].
- [2] Optimus Learning, "The Advantages and Disadvantages of BYOD," Optimus Learning, 4 September 2013. [Online]. Available: <https://www.optimuslearningservices.com/practical-ld/advantages-disadvantages-byod-in-learning/>. [Accessed 04 May 2019].
- [3] M. Rouse, "mobile device management (MDM)," November 2017. [Online]. Available: <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>. [Accessed 4 May 2019].
- [4] Comtact Ltd., "5 BENEFITS OF IMPLEMENTING A MOBILE DEVICE MANAGEMENT (MDM) PLATFORM," Comtact Ltd., 12 January 2018. [Online]. Available: <https://www.comtact.co.uk/blog/key-benefits-of-implementing-a-mobile-device-management-mdm-platform>. [Accessed 04 May 2019].
- [5] VMWare AirWatch, VMWare AirWatch, [Online]. Available: <https://www.air-watch.com/capabilities/mobile-security>. [Accessed 04 May 2019].
- [6] "Top 9 MDM (Mobile Device Management) Solutions 2017," 2017. [Online]. Available: <https://iactivate.host/top-9-mdm-mobile-device-management-solutions-2017/>. [Accessed 04 May 2019].