

Internet Technology and Security

Synthesize a solution to a potential real life scenario

Reka Ragupathy
RAG16831638

Table of Contents

1. Advantages and disadvantages of BYOD
2. Different types of policies
3. Bibliography

Advantages and disadvantages of BYOD

Before we start, we should know what BYOD exactly means. It stands for 'Bring Your Own Device' and what it means is that employees can bring their own mobile devices such as smartphones and tablets and on their own device they are allowed to access confidential business data such as databases and email. So it is easy to remotely access this information even if the employees are outside the office. Employees can also learn from outside like home using eLearning modules. The main important thing is that the BYOD – Bring Your Own Device is your own and not the companies.

ADVANTAGES

- **Lower Costs**

The main benefit to the company is that the company doesn't need to buy costly devices for the employees to do the eLearning. An average tablet price will start from £150, so an eLearning plan including 300 employees can cost you around £4500 before any training has even been purchased. If the company doesn't need to buy any devices, that means enough savings. The fact is that people take more care of their own equipment than company-owned devices and if the repair cost is also employee's. So, it can reduce companies' breakages and wastage and can save money again.

- **Technology Familiarity**

Most people feel familiar with their own devices. For example, who uses Apple products, they feel comfortable with Apple technology and who uses Windows products, they are better with Windows operating systems. It can be very annoying for an employee to use a different device. BYOD take this issue away.

- Flexibility

Employees does not need to travel with plenty devices to do home and work needs because the one device will fulfil both. The work that usually can be done only in the office can be done anywhere anytime they want. Finally, employees are not hindered by the usual strict rules that they have to adhere to when using company property. To your workers, BYOD allows greater freedoms.

DISADVANTAGES

- Costs for the employee

The employee needs to take the costs of BYOD as mentioned before. Not everyone wants or have such a device. If the company told the workers to get one for work is likely to leave them feeling fairly hard done by. The increased usage and transportation of the device likely leading to quicker depreciation of the device and possible accidents. So the repairs cost will come to the employee again. The employee will not be happy to take all the cost in their shoulder.

- Device Disparities

The employer or the company have the full freedom to buy the matching device for their employees. The device will have then the suitable technological features for the need they are serving. However, if the employee chooses their own BYOD, it will be all with different capabilities and different operating systems that again will run different programmes at different levels of quality. Nowadays, it is really not easy to get programmes that are good in quality but also same time, it needs to cover all platforms and realistic quality of devices. Another reason is also that the systems need to be adapted to be able to deal with BYOD policy.

- Security

If it comes to data leakage or if viruses catch the system, it will be a huge loss for the company and they can't afford that to be happen. That's why

companies spend a very huge amount of money on their security systems. This level of security an employee can't have it. At the same time as the everyday security software for home use can cover all day to day activities, you might not trust them to be up to the job of protecting your valuable customer data. Also, how can a company stop employees who are leaving the company and they have all the important company data on their device? And also, from the view of an employee, their privacy is also at risk because if they do any personal web surfing on a device which is linked to their company's systems.

Different types of policies

Security policy

- Use password protected access controls:
To access the devices or account, you should give a strong, unique, secure password or PIN for each of them so that cannot be guessed easily.
- Control wireless network and service connectivity:
You should turn off the Wi-Fi and Bluetooth when not in use, and employees should only connect to trusted networks with their devices. Before connecting their devices by mistakenly to unsafe networks, you should set your devices so that they will ask for your permission before they connect.
- Control application access and permissions:
You should set the app application settings so that each application can access only what it needs to function and nothing more.
- Keep OS, firmware, software, and applications up-to-date:
You need to make sure that the devices' OS and other software are updated in real time.
- Back up device data:

.....

Bibliography

- <https://www.veracode.com/security/byod-security>
-