Research Paper Technology

Bring Your Own Device (BYOD)

Sanjay G Kulkarni | National Informatics Centre-SDU, Ganeshkhind Road Pune

KEYWORDS

Bring your own device(BYOD) which is also known as Bring Your Own Technology refers to the policy of permitting employees to bring personally owned mobile devices(laptops, tablets and smart phones) to their workplace and to use those device to access privileged company information and applications. The term came in common use in 2009 courtesy Intel.

Large number of organizations are now starting implement BYOD initiatives. Today people read their emails, chat with friends , modify spreadsheets, communicates with the vendors and customers using the company information with own device. According to recent symantec survey 59% of enterprises are making line of business applications accessible from mobile devices in an effort to increase efficiency , increase workplace effectiveness and reduce time required to accomplish task.

Advantage

- **Enhance the productivity :**

The mobile devices offer convenience and speed . A sales executive can for eg. Update the spread sheet , send email , update the document while travelling at any time from anywhere.

- **Cost Saving :**

Many employee prefer to own the device of there like and since it is purchase and owned by employee there is cost saving on the company behalf.

- **Improve Morale :**

Allowing the employees to use their own device gives satisfaction with the work and company.

- **Updation of the device with the technology.**

The technology keeps changing and updating the device with the new technology is many a times not possible to the company which can be achieved with the frequent updates by employee.

Disadvantages

- **Security**

The number one concern is about the data security. There could be data leaks which would help the business rivals.

- **Loss of the Device**

The data loss due to the loss of Device could be cause of concern which not only is loss of the personal data but important data of the company.

- **Employee Leaving Company**

In case the Employee leaving the company or becomes the companies competitor the data cannot be retrieved.

- **Restrictions on Device usage:**

The company can impose the restriction on the usage provided if it is owned by the company but the same cannot be imposed for employee owning .

According to Avalande's survey latest findings 88% of the executives have reported that the employees are using personal technology at the workplace . As per the Gartner prediction 70% of the mobile workforce will use hybrid/tablet device by 2018. There is a need to follow the best industrial practices in order to overcome the constraints of taking full benefits of the technology. The organization should have BYOD policy in place which at minimum should have strong password policy. The propriety right policy on the company information which belongs to should be returned to the company before leaving the company should be stated. On the technology front Mobile Device Management software solution(MDM) offering various levels of control which force compliance with the user .The public storage access google cloud with the restrictive necessary privileges given to the company may safeguard the data even if the employee leaves the company or device is lost.

In the recession period or otherwise the organizations may think of the solution of cost cutting with other advantages with the trend of BYOD with the strict adherence to the policies and framework designed by it.