



Article published on July 30th 2012 | [Technology](#)

Many CIOs (Chief Information Officers) look back to the early days of enterprise mobility as the good old days, when things were just so much simpler for them. There were few mobility devices and fewer platforms, which made it much easier to implement security solutions. Most of the enterprise employees were baby boomers and the attempts to circumvent company security were much fewer. In those early days, the mobility devices were mostly company owned and provided to the employees for carrying out the company's work. The cost of buying and maintaining such devices was considered to be a necessary evil by most companies in those days. At that point, few people could have predicted that there was a storm coming.

The storm came with the introduction of the first Apple iPhone, intensified with the advent of devices powered by Google's android and the whole enterprise mobility landscape started to change at a rapid pace. The availability of iPhone and Android powered devices, which were capable of accessing data on the organizational network, led the IT department of many companies to reassess their current strategy and decide on a suitable course of action to preserve the integrity of sensitive corporate data, while simultaneously ensuring that the cost incurred by the organization while minimal. At this point of time, the first BYOD policy was suggested by a number of leading IT individuals.

BYOD, an acronym for Bring Your Own Device, provides various benefits to both the organization and its employees. Key BYOD benefits include:

- Reduced cost to the company as most of the cost is shifted to the users
- Increased employee mobility
- Greater employee efficiency and productivity
- Increase in overall employee satisfaction
- Simplified IT infrastructure
- Reduction in ongoing end-user device management, troubleshooting and support
- Allows organizations access to latest features incorporated into mobility devices
- Increased frequency of hardware upgrades by users ensures availability of up-to-date devices
- Allows IT department the freedom to focus on various strategic initiatives
- The training time for new devices is also reduced

Despite of the various benefits of BYOD as mentioned above, there are many emerging concerns related to introduction of BYOD in an enterprise setting. Key concerns related to organizational implementation of BYOD are:

- Reduced organizational control over IT hardware
- IT department's control over use of IT devices is reduced

- â€¢ Increased risk of non-compliance with industry norms such as PCI DSS, HIPAA, or GLBA
- â€¢ Difficulties in ensuring uniformity of security protocols across devices and platforms
- â€¢ Ensuring corporate data is segregated and retrieved from employees leaving the organization
- â€¢ Difficulties related to ensuring adequate protection of sensitive corporate data
- â€¢ Reduced network protection against malware
- â€¢ Problems related to installing, managing and supporting client security software
- â€¢ Bandwidth problems due to availability of multiple devices

Such problems have caused CIOs of many companies to spend sleepless nights, while IT departments have worked round the clock to resolve or circumvent such issues. Some of the best practices with respect to BYOD are discussed here.

### Limiting the Devices and Software in use

The IT department can help protect corporate data by controlling the devices and software used by the employees to carry out their work. Though such actions can possibly lead to reduction of employee satisfaction, but it ensures that sensitive corporate data is secure and compliance is maintained. Control on software use was recently introduced by IBM with respect to the use of Appleâ€™s Siri and Dropbox utility. As both software store data on 3rd party servers, the risk of sensitive corporate data being accessed by unauthorized individuals is increased. By applying limits on the devices suitable for office use by employees, the BYOD policy attempts to limit the number of software capable of being utilized on the company network, including potentially unwanted firmware inbuilt into some mobile devices. Many offshore development companies in India help enterprises choose which devices and software are suitable for use in specific enterprise situations.

### Increasing Awareness among Employees and Configuring of Devices prior to Enabling Access

The IT departments of companies with either new or existing BYOD policies also need to introduce programs, which generate awareness among employees about how the use of unauthorized software/devices can harm the companyâ€™s network to improve overall employee compliance. IT departments also need to configure devices with security features such as remote wipe or install security software even before the mobility device connects to the corporate network. Such measures are designed to provide additional security of company data in the eventuality that a mobility device is lost or stolen.

### Restricted Network Access

Before allowing BYOD policy devices to access corporate networks, it is also advisable that the network access of such devices is decreased by the use of network pass codes, firewalls and other measures. Companies with long-term expertise in developing such security solutions help ensure compliance with all currently enforced local as well as international data security norms. By restricting network access through introduction of advanced security solutions, organizations can protect sensitive data by further reducing the possibility of unauthorized access.

### Effect on the Enterprise Mobility Market

As more and more organizations adopt the BYOD approach, newer methods of ensuring data security are expected to emerge. However, one thing is for certain- the BYOD approach is here to stay and organizations will have to devise various strategies to ensure that the BYOD policy does not adversely affect the interests of the company and all local as well as internationally applicable

compliance is maintained. Newer and more advanced security solutions are also expected to emerge as concerns surrounding the BYOD trend intensify. More organizations are also projected to move towards composite systems in order to integrate a rising number of mobility devices into their enterprise networks. These are just a few of the changes which we expect to see in the recent future and more changes are expected to occur regarding how companies operate and tackle the BYOD trend in the recent future.

Article Source:

<http://www.articleside.com/technology-articles/byod-and-its-impact-on-enterprise-mobility.htm> - [Article Side](#)

[Dipak Chopra](#) - About Author:

Dipak Chopra has over 15 years of industry experience and is a leading figure in the information technology industry. Prior to joining eXtendCode, a software development company based in India, which provides Web Enabled Solutions, a [Mobile Solutions](#) etc. Dipak worked at management positions in different global companies.

To know more about us Click here a [software development india](#)

Article Keywords:

mobility devices, enterprise mobility,byod policy, mobile solutions, security solutions

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!