Bring Your Own Device
BYOD: Optimised in 10 Steps
Table of contents

Introduction .......................................................................................................................... 3
Advantages and disadvantages of BYOD ................................................................. 4
Advantages ..................................................................................................................... 4
Disadvantages .............................................................................................................. 4

BYOD Optimised in 10 steps ......................................................................................... 5
Step 1: Analyse the employees .................................................................................... 5
Step 2: Draft a BYOD policy .......................................................................................... 5
Step 3: Ensure data security and integrity ...................................................................... 6
Step 4: Draft a pilot programme ..................................................................................... 6
Step 5: Evaluate technologies ....................................................................................... 7
Step 6: Establish self-service ......................................................................................... 7
Step 7: Keep the total cost of ownership (TCO) in mind ............................................. 8
Step 8: Select applications ............................................................................................. 8
Step 9: Monitor user behaviour ...................................................................................... 8
Step 10: Prepare support and help desk ....................................................................... 8

Conclusion ....................................................................................................................... 9
About the author .............................................................................................................. 9
Introduction

When you consider the current IT trends in detail, one trend dominates: cloud computing. And in the context of cloud computing the topic “Bring Your Own Device” is in the headlines again and again. Although both topics have nothing to do with each other directly, both are somehow always related in context. Due to a lack of legal regulations, this trend has so far not really prevailed in Europe. Moreover, many CIOs often cite data security as a reason not to use BYOD programmes. But technical possibilities are quickly outpacing existing concepts. Whereas it was previously unthinkable that private devices and systems could be integrated into a company’s infrastructure, this trend has nevertheless gradually found its way into companies. The usual “door opener” is the Apple iPad, which especially C-level manager often like to use. Meanwhile, many employees also use personal smart phones or notebooks professionally. Even if not yet officially supported, in most cases these devices are at least tolerated by the IT department. Even the European Parliament is planning to officially introduce the use of iPads for its members.
Advantages and disadvantages of BYOD

Employees’ private lives are increasingly influenced by new technical devices which they also want to use professionally at work. A trend that - according to the technology research company Gartner - will bring more changes to business IT than the last ten years. But where there is light, there are also shadows. Therefore, the advantages and disadvantages of a “Bring Your Own Device” programme should be carefully considered.

**Advantages**

- Makes smart phones, tablets, and other current consumer devices powerful business tools, thus increasing productivity and employee satisfaction. Meanwhile, there is hardly a consumer device which doesn’t offer email and web access.
- Enables fast and secure access to corporate applications and resources regardless of the employee’s location and time zone.
- Reduces costs and facilitates IT management of devices.

**Disadvantages**

- Data security and IT compliance: who actually owns the data on personal devices, e.g. what happens when an employee leaves the company?
- The corporate infrastructure needs to be protected against malicious software on private devices.
- Productivity must be maintained when a device is lost or needs to be repaired, e.g. through support contracts or replacement.
- Increased costs and demands on the existing infrastructure through standardisation, virtualisation and remote access solutions.
How can you introduce a BYOD programme to your company and profit from its decisive advantages - despite all known and existing disadvantages?

**BYOD optimised in 10 steps**

The following ten steps can help to successfully implement a BYOD programme. Of course, not all steps are suitable for each type of business or employee; even the order of the steps is not set in stone. However, the general direction is certainly universally applicable.

**Step 1: Analyse the employees**

A BYOD programme is not suitable for every employee in the company. No employee should be selected who works with important and mission critical data. Employees who belong to the initial users of mobile devices (early adopters) should first be grouped together in the form of a pilot project. These include, for example, employees of the IT department, sales and marketing personnel as well as software developers. This selection ensures valuable results about the expected benefits. It is aimed at employees who have an extensive technical understanding of the underlying technology (IT), or travel a lot and need mobile access to data (Sales and Marketing). Employees who need to access large amounts of data at any time of day (software developers) should also be taken into account.

Another aspect is the age group. Younger employees are usually very receptive to a BYOD programme, whereas older employees generally prefer the “managed client computer” and may feel overwhelmed by another device.

**Step 2: Draft a BYOD policy**

A guideline for the use of private devices within the company is essential. All departments (HR, Legal, IT) need to sit down together and establish rules for the use of corporate data on personal devices. In addition, the ownership structure must be described in detail. Who owns the social network data or accounts when
they’re used professionally and perhaps even paid for by the company? It is particularly important to precisely define whether and to what extent the employee may be held liable for loss of data. A similar agreement should already exist for companies that already provide their employees with notebooks. It has always been a balancing act to specify what employees may and may not do with the company notebook. In addition to private use, which is usually prohibited, some additional software not available in the standard portfolio may need to be installed for business use. Many companies have already established guidelines for local administrator rights that have been in use for some time.

Step 3: Ensure data security and integrity

In all cases, protection and integrity of critical business data must be given top priority. Technically, the protection and integrity of business data has been realisable for some time through the use of encryption. Appropriate products are available on the market in almost all price ranges. So this should not be a new issue for companies that already provide their employees with mobile devices (smart phones, notebooks etc.) for professional use.

However, one must keep in mind that in a BYOD programme the employee’s private data on the device must be protected from company access. It is absolutely necessary to conclude appropriate agreements with employee representatives that are acceptable to all parties.

Step 4: Draft a pilot programme

It has always been a good idea to involve the staff as early as possible in any process. An ideal start for a BYOD programme is a pilot programme with selected employees in a test or development environment. The findings from such a pilot programme provide valuable results for further implementation, and also offer comparative figures for scaling up the programme, as well as for schedules and budgeting plans for the productive implementation.
Step 5: Evaluate technologies

The evaluation of applicable technologies could fill books. Here, I would like to just limit myself to the essentials. Looking at the areas of total cost of ownership (TCO), security and usability, another buzzword offers the best values: Here we are referring to virtual desktops. In this area, all three major vendors - Citrix, Microsoft and VMware - offer solutions that are perfectly suited to a BYOD programme. Virtual desktops or applications published via terminal servers are operated in your own data centre (or as an SaaS offering in a cloud data centre) and can be displayed on private devices - protected with the appropriate data security technology. When considering costs, the terminal server achieves the best TCO results. Virtual desktop infrastructures are somewhat more expensive, but they provide more features and flexibility. Both technologies have one thing in common: services are rendered in the data centre, and to all intents and purposes business data does not leave the company. The disadvantage is that this technique can only be used with a network connection. Currently, there are opportunities for offline use, however the corresponding data must of course be physically present on the device. Naturally, the data should be secured via encryption. The technical options available on the market (client hypervisor, application streaming etc.) offer a host of additional products to implement a BYOD programme. Important at this point is not only a thorough test of the solution in a pilot environment but also a look at the costs (see step 7).

Step 6: Establish self-service

To make the installation of enterprise software on private devices easier, self-service could be introduced. This way, a user is able to install or remove the required software himself with a suitable tool. For licence management purposes, the assignment should be entered into a workflow and approved by the supervisor prior to deploying the software.
Step 7: Keep the total cost of ownership (TCO) in mind

As with any project, the costs must also be considered. If you really wish to save 40% of the cost of procuring devices (as previously mentioned), you should also consider the infrastructure costs. If the appropriate infrastructure (virtualisation, additional servers, access solutions) needs to be created within the company, a BYOD programme may no longer be seen as a good investment. However, a business case for the virtualisation of desktops will pay off when standardising (golden image) the managed devices. In this case, nearly all vendors offer relevant TCO and ROI calculators. Additionally, the cost of mobile phone contracts is an issue that necessitates expense management in the company.

Step 8: Select applications

Another important aspect of such a scenario is the number of applications used. Not all applications can be placed on private devices by using established technologies. Many applications require a physical installation, which for example is only possible to a very limited extent on a Mac OS computer, especially since support expenditures are also incurred when installing these applications. In any case, review the applications to determine which ones are not suitable for such a BYOD programme. You may perhaps be able to utilise alternative applications or switch to web-based applications.

Step 9: Monitor user behaviour

The saying “Trust is good, control is better” applies here as well. Use suitable tools to ensure that your users comply with the stipulated guidelines. The company, not the employee, is primarily liable for violations of data protection laws (see steps 2 and 3). Just as important as compliance with security policies is the respective performance data. Again, using the appropriate tools, care must be taken that the infrastructure also meets the needs of the employees.

Step 10: Prepare support and help desk

Train your user help desk. Your help desk employees will need to cope with any number of exotic problems, especially in the early phase. For example, it must be determined how problems such as “Since I’ve installed xyz, my private Twitter client doesn’t work any more” are to be handled. The help desk needs to attend to these problems, especially during the implementation phase, and also has to deal with other operating systems, such as Linux or Mac OS. Ensure that the help desk staff also has some of the more common devices on hand for testing purposes. Also, support solutions in the cloud, e.g. Citrix GoToAssist, have proven to be helpful and provide remote support for mobile users.
Conclusion

Allowing employees to choose their preferred device and access corporate data from any location can lead to an immense increase in productivity. The main advantages are not only employee satisfaction and increased productivity and creativity, but also a long-term reduction in IT support costs. Through the use of available technologies and best practises, the needs of end users and the corresponding support of the IT departments contribute equally to a successful implementation of a BYOD programme.

About the author

Thomas Krampe is an IT architect, virtualisation evangelist and author of several white papers, articles and blog posts. With more than 15 years of professional and project experience in large corporations and global consulting firms, he was honoured in 2009 by Citrix as a Citrix Technology Professional, a select group of currently 43 persons worldwide. Thomas Krampe is currently head of the Virtualisation & Cloud Competence Center of Bechtle GmbH & Co. KG in Mannheim, Germany. He also gives lectures and presentations at many Citrix Systems Inc. sponsored events, including Citrix Synergy in the USA and EMEA as well as the Citrix Geek Speaks in Germany, Austria, and Switzerland.
Resources for achieving business agility
For more white papers, case studies and on-demand webinars, visit www.gotoassist.co.uk.

Citrix GoToAssist
Our Citrix online service for remote and customer support as well as IT monitoring

Get your free trial version:
United Kingdom: 0800 011 2120
http://www.gotoassist.co.uk