BYOD ASAP? Not So Fast.

Why Bring Your Own Device Might Not be Right for Your Company

Have you gone BYOD yet? If you believe the fervor in the media and some business circles, it's nothing less than a cost-saving, productivity enhancing panacea that will give your bottom line a big boost. But is Bring Your Own Device (BYOD) really the best way to manage the mobile devices your employees use for company business? It is easy to understand why the BYOD concept would have a lot of appeal to cost-conscious occupants of the C-suite, but as usual, there is more to the story than is apparent on the surface. Cost savings may not be what they appear, and there can be numerous other pitfalls that more than mitigate the potential benefits. BYOD may be right for some, but companies need to carefully consider all the associated issues.

What Is BYOD?

BYOD stands for Bring You Own Device to work. It is a relatively new and growing trend of allowing employees to use their own mobile devices, such as smartphones, tablets, notebooks, etc., to do company business, connect with its networks, access its data and more. The primary benefit of BYOD is obvious. Allowing workers to use devices they own saves the company money – potentially a lot of money. For many business leaders, that was all they needed to know before diving in and reversing their long-held policies of only allowing company-owned devices to connect to networks and access data.

Allowing Access vs. BYOD Only

It is important to recognize the difference between policies that permit employees to use their devices for work (while still supplying company-owned devices) and policies that require workers to exclusively use their own smartphones, tablets, laptops, etc. (whether the company pays for all, part or none of the cost). Both policies can create serious concern about security, compliance, control and other issues, but BYOD-only policies are more extreme and can be much more difficult to address. It is far simpler to put effective safeguards in place that deal with limited use of employee-owned devices than in a BYOD-only environment.

A Growing Trend

According to data from a variety of studies, the concept is popular and growing. IBM found that 73% of business leaders surveyed allow BYOD. An Eset study showed that 81% of US adults use a personal device for work-related functions. Cisco sited a study that showed that 95% of organizations surveyed allow employee-owned devices in some way in the office, and 36% provide full support for employee-owned devices.

These statistics do not indicate that a large majority of companies have gone to a BYOD-only policy; just

that they allow employee-owned devices to be used for work. That is a big difference. However, more companies are adopting a BYOD-only policy every day, eliminating business-owned devices. The forms range from subsidized BYOD, where the company gives employees a monthly stipend to contribute to the cost of the devices and wireless plans, to zero-compensation situations where the workers absorb all the cost themselves. Surprisingly, 50% of companies with BYOD are requiring their employees to pay all the costs and there is little push-back from the workers (Good Technology State of BYOD Report, 2011). The assertion is that employees like choosing and working with their own devices so much that they are willing to foot the bill – completely.

Moving Too Fast?

Like most hot new trends, BYOD has gained its own momentum and accelerated to a fever pitch in record time. Why not? It appears to save a lot of money and employees like it. But has it gone so fast that businesses have neglected to consider all the issues? The answer is quite probably yes. There are real concerns in a variety of areas from security to ownership and access rights that are making prudent business leaders take a careful look before leaping. For example, after implementation of a BYOD policy, IBM has imposed strict limits on what applications can be used, including Dropbox and the iPhone's Siri, voice activation feature. There is much to consider.

The Pros of BYOD

- **Potential Cost Saving** – employee-owned devices can reduce or even eliminate the company's cost for mobile devices and service plans.
- **Worker Satisfaction** – employees are happier and work more using devices they like.
- **Employee Productivity** – research suggests that workers who use their own devices tend to work more hours and more productively.
- **Newer Technology** – employees tend to upgrade devices more often than companies, making the latest features and capabilities available.

The Cons of BYOD

- **Security** – this may be the biggest down side to BYOD. Without control of the devices, applications and usage on its network, a company cannot ensure the security of its data and systems. About 1.3 million cellular phones are stolen each year and over half of stolen laptops result in data breaches. Recent Proofpoint research revealed that more than 1 in 5 of US companies surveyed (22%) investigated the exposure of confidential, sensitive or private information via lost or stolen mobile devices in the previous year. 51% of respondents are highly concerned about the risk of information leakage via email sent from mobile devices. In another survey, PwC found that 82% of large organizations reported security breaches caused by staff. Only 39% of large organizations encrypt data downloaded to smartphones and tablets.

- **Cost Savings** – on the surface it looks good, but when you consider the indirect and hidden costs, savings may not be realized. In one study, the Aberdeen Group found that BYOD costs companies 33% more, on average, than a company-owned policy. Added expenses come from policy administration, monitoring, added security precautions, training, ensuring that systems accommodate many devices and platforms and other issues.
- **Usage Policies** – it is difficult for a company to tell its employees what is acceptable usage of their own devices. Personal activities can become inextricably mixed with business functions, which can negatively reflect on the company.
- Number Ownership – if an employee leaves, so does his/her phone number. This can be a big loss if the employee has many customer and vendor connections. It can also cause liability and public relations issues.
- **Data Protection** – maintaining control of data that resides on employee-owned devices is nearly impossible. In addition, retrieving and extracting proprietary data and other information from devices when an employee leaves can be very difficult.
- **Compliance** – compliance regulations, such as HIPAA, PCI DSS, GLBA, etc., can be much harder to meet when a company does not own the devices its employees use.

- **HR Issues** – no access to employees' devices, invoices and calling records makes it more difficult to monitor work activities, policy compliance and other behaviors.
- **Employee Satisfaction** – while some employees are initially happy to be able to use the devices they prefer, even if they have to pay for them, many are not, and this may change as they see the cost adding up. In addition, a prudent BYOD system will require regulations and monitoring of employee-owned devices that may not be well received.

How to Decide if BYOD is Right for Your Company

No two businesses are the same, so each must do its own analysis to decide whether BYOD is the right course to take. Consider the following:

- How important is network and data security to your company?
- Can your existing security systems accommodate BYOD?
- Can your IT and administrative structure support BYOD?
- Is your company culture right for BYOD?
- Does your company have to deal with compliance and regulatory issues?
- Have you considered all the indirect and hidden costs of converting to BYOD?
- Do you want a subsidized or zero-contribution BYOD policy?

GRUDI
A S S O C I A T E S

Innovative Solutions
Simplified Telecommunications

1044 East Main Street, P.O. Box 626, Palmyra, PA 17078 ▪ Office: 717.838.5022 ▪ Fax: 717.838.5086
www.grudiassociates.com

Voice & Data
Wireless
Managed Solutions℠
Enhanced Solutions
Hosting Services

If You Do Adopt BYOD

After careful consideration, if you choose to go with a BYOD policy, you should also consider the following:

- **VDI** – a hosted Virtual Desktop system can help alleviate many security concerns, compatibility issues and other potential pitfalls. VDI moves most critical applications and data to a cloud-based server so they will not reside on vulnerable devices.
- **Test First** – before diving in to BYOD for your entire organization, create a pilot test of a small, representative group of employees to see how it works and if it delivers the benefits you expect.
- **Get Help** – a telecom expert can assist with the planning, implementation and monitoring of your BYOD initiative. An outside perspective can be invaluable.

Summary

BYOD is an intriguing concept that promises cost savings and added productivity at a time when businesses are looking to improve their bottom lines any way they can. Preliminary studies and anecdotal information further suggests that employees like the idea, so why not jump right in? Perhaps the answer is the age-old adage: "If it looks too good to be true, it probably is." BYOD may be right for some, but the exaggerated cost savings, security concerns, compliance issues and other pitfalls are very real. Making an informed decision takes information and careful consideration. Do your homework or get expert help on BYOD ASAP.

GRUDI
A S S O C I A T E S

Innovative Solutions
Simplified Telecommunications

1044 East Main Street, P.O. Box 626, Palmyra, PA 17078 ▪ Office: 717.838.5022 ▪ Fax: 717.838.5086
www.grudiassociates.com

Voice & Data
Wireless
Managed Solutions℠
Enhanced Solutions
Hosting Services