Is BYOD Right for Your Business?

Have you gone BYOD?

If you believe the fervor in the media and some business circles, it's 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, but as usual there is more to the story than what is apparent on the surface. Cost savings may not be what is expected, and there can be numerous other pitfalls that might mitigate the potential benefits. BYOD may be right for some, but companies need to carefully consider all the associated issues.

What Is BYOD?

Bring You Own Device to work has been a controversial concept for many years. BYOD allows employees to use their personal mobile devices, such as smartphones, tablets, notebooks, etc., to do company business, connect with its networks, access its data and more. An ESet study showed that 81% of US adults have used a personal device for work-related functions. The growing number of employers who require employees to be more accessible while on-the-go is a big contributing factor.

However, according to a study conducted by BitGlass, 57% of employees do not want to participate in BYOD, especially if an MDM (Mobile Device Management) Solution is in place. An MDM is a system that helps companies manage or control features, functions and data options on mobile devices. Examples of MDM functionality include the ability to wipe the device remotely, ensure the phone has a PIN or passcode, block the device from downloading any applications and even push out to personal devices specific applications employees need in their jobs.

While an MDM is crucial if a company is considering BYOD, it also presents a new set of challenges and concerns. Employees may feel they have no control over their phones and that MDM and associated policies are invasive. Many companies appropriately see this type of control as necessary for protecting sensitive information and IT systems. Both of these concerns are valid and must be considered.

The Pitfalls of the Positives

Often, the positive aspects of BYOD can also be drawbacks. For example, employees tend to upgrade devices more often than companies, making the latest features and capabilities available. However, new software updates and features are prone to bugs, incompatibility issues, and may even render the device nonfunctional until a more stable version is released.

Another example is employee satisfaction. Most employees like the fact they do not need to carry two devices. However other employees may feel having one device that combines work and personal numbers is disruptive to their delicate work-life balance. Also, IT departments have the additional burden of accommodating and working with an array of device models. Troubleshooting with multiple software versions, operating systems, apps, models and manufacturers is difficult and can become a time sink for the IT department.

Ownership and Security

The biggest downside of BYOD is the loss of security and ownership, for both the company and the employees.

With cellphones, the ownership of the number is either with the company or the employees. When a number is the property of the company, employees who end their employment may lose the number they use for their personal life. Alternatively, if the employee owns the number and leaves, the company would lose a number that clients and others know. Because exiting employees often go to competitors, this can translate into a loss of business, as client calls follow that employee. There can be a wide range of liability, legal and public relations issues.

BYOD can also be a huge security risk. Employees download and view sensitive company documents and data onto their personal devices, which may not be secure or comply with regulatory organizations such as HIPAA, PCI, DSS, GLBA and more. An MDM solution is vital to maintaining complete control of the device and ensuring it has security authentication methods. This is essential for preventing the download of malicious applications and making sure the device can only connect to company approved networks. If the device poses a security risk – being lost, stolen, removed by a past employee, etc. – the company can remotely wipe all data from the device. The employee's personal pictures and content would be deleted along with company information, which can result in conflict. It is important to know that an MDM solution must be actively managed and maintained or it will not be effective.

The Costs of BYOD

On the surface, BYOD looks good. There are no devices to purchase, no plan to pay for, and giving each employee a stipend amount toward their personal cost may seem cost effective. However, subsidizing BYOD often exceeds the per employee cost of providing phones, especially in a larger company. In many cases, BYOD significantly increases the cost per device. In a Grudi Associates client case study (see below), the company was paying a $100 stipend per employee per month. When BYOD was eliminated, the cost was reduced to $58 per line. Additionally, the company is able to take advantage of special device pricing, bill credits or any buyback programs that are available, which further lower costs.

The "soft costs" can also be significantly underestimated with BYOD. Some businesses view BYOD as a hands-off concept, thinking it will save time because they "don't have to deal with the devices." This is a huge misconception. In fact, it can create an immense strain on several different departments. The IT department workload increases due to troubleshooting time. BYOD makes it very difficult, if not impossible for the HR department to monitor work activities, obtain call records, ensure policy compliance and address other issues. The accounting department must spend extra time and resources identifying and tracking expenses that need to be billed to the correct employee, since most bills do not separate these charges.

In addition, there are added expenses related to policy administration, MDM solutions, monitoring, added security precautions, training and ensuring that systems accommodate many devices and platforms.

Case Study

Following is an actual example of how eliminating BYOD benefitted a Grudi Associates client:

A full-service community bank had BYOD in place for 5 years.

- They implemented BYOD under the impression that they could save money.
- Employees thought it would be convenient to only carry one device.
- Static monthly stipends were paid to each employee using their device for business communication.
- When an employee left the company, clients would still call that number.
- The bank utilized an MDM solution to help control security, but even with policies in place, they remained out of compliance and violating FDIC policy.
- Employees were spending more than the stipend on their personal accounts and were unhappy with the stipend amount.

Is BYOD Right for Your Business?

Grudi Associates recommended termination of the BYOD program and provisioned new company phones and numbers for the employees. Grudi Associates also provides outsourced management, enabling the bank to be back in control of its phones and usage. The results are a 40% cost reduction, company-selected standard devices for troubleshooting ease, ownership of all the numbers used in their business and FDIC compliance.

Conclusion

If you are considering BYOD, there are many important considerations. Properly implementing BYOD must involve an MDM solution, such as Airwatch or MobileIron. Careful planning and implementation are necessary, since BYOD is not as “hands-off” as some think. It can be time consuming, expensive and a serious risk to data, information and systems. BYOD may be right for some, but for most companies it is best for employees to use company devices. Enlisting the help of a telecom and IT expert for the planning, implementation and monitoring of a BYOD initiative is a good idea. The same is true when moving away from BYOD entirely. Contact us for more information or assistance.

© Copyright Grudi Associates, 2018. All rights reserved.