An IT Manager's Guide to BYOD Benefits and Risks

Save your company money and make employees happier at the same time!

More than ever, employees are bringing their own personal devices to work. According to Forrester Research, 53% of employees use their own devices at work and this trend can pay off for your business by adding as many as 240 productivity hours a year for each mobile employee. However, before your company decides to implement a BYOD program, there are risks and benefits to consider.

BYOD Benefits: Save the Company Money, Appease Workers

One of the main reasons businesses opt for a BYOD program is to make their employees happier. When an employee can work from and use a device of their own choosing, it is more enjoyable than being forced to use a device they are not comfortable with. Happier employees are also usually more productive employees, so this is a big benefit.

Another benefit is the cost savings of not having to supply employees with corporate phones as well as the support for a mobile and cloud-focused IT strategy, which allows employees to access their work from the cloud, meaning more productivity.

BYOD Privacy Issues and Other Concerns

With a BYOD program, companies can track the activity of their employees on their personal devices, delete personal data and see the user's Web activity. Although having more control over employees' personal devices might make businesses happier, employees are generally not as thrilled.

To help preserve BYOD privacy, IT can use secure containers or Mobile Device Management (MDM) systems that keep personal and work data separate, monitor data with Mobile Application Management (MAM) or Mobile Information Management instead of managing devices, or set up virtual desktops or phone lines for BYOD access. However, whichever strategy you decide to use, it needs to be clear to your employees what they are in for.

4 Big BYOD Risks to Consider

Now that you have some ideas of the benefits of BYOD, there are also some risks to consider about implementing a BYOD program.

1. How will you pay for the service on employees' personal devices?
2. How will you draft acceptable use and security policies that include the consequences of violation?
3. How will you train users and help desk staff on best practices and support?
4. How will you handle BYOD security?

How to Minimize BYOD Risks

Security is one of the biggest issues to consider when implementing a BYOD program. Although the security risks can seem overwhelming, there are ways to keep data locked down and your business secure.

Policies and procedures are the first line of defense against data leaks; however you need your employees to adhere to these policies and procedures for them to be effective.

To mitigate risks when employees do violate policies, make sure to control data and network access with two-factor authentication and use the right tools to managed devices, applications and information.

Encrypting data will also help to keep corporate information safe, and will also encourage your employees to use the virtual private network.

Make Sure Your BYOD Policy Has More Pros than Cons

There are a number of BYOD benefits and risks, often more than we realize. Whenever your business is looking to implement a BYOD program, it is helpful to write down the pros and cons of the program and see if it is beneficial to your business strategy.

To learn more about Bring-Your-Own-Device programs and how they can benefit your business, please contact Intega IT at (613)260-1114 or by email at sales@intega.ca.