Benefits, Risks, & Solutions Of Implementing BYOD Policies

Dean Wiech, Managing Director, Tools4ever

A new trend gaining speed in many industries is the concept of “bring your own device” (BYOD). Plainly put, BYOD is when employees have the ability to bring their own technical devices - like smart phones, tablets and laptops - and use the company’s network instead of a company-provided device. BYOD has many benefits and risks, though, that each organization’s IT department needs to consider.

Benefits

Increased Productivity

The use of technology at work has increased significantly over the past few years as using paper and manual processes continue to decrease. In education, for example, schools have increasingly taken to using technology in the classroom by providing students with tablets and computers. Recent research has shown that this type of learning allows students to be more interactive and engaged in the learning process. In business, the use of technology has increased because of green practices and organizations realizing that by positioning themselves as environmentally friendly they are saving money and generating external support of their efforts. Though technology increases overall productivity, research also shows that employees are even more productive if the device they use is their own.

Lower Cost to the Company

Though the use of technology is a benefit to employers as it without a doubt makes employees more productive, the cost to companies that purchase a large number of computers or tablets is a tremendous financial commitment. Most of the technology used by organizations is only current and up to date for a certain, limited period of time and then becomes obsolete and in need of replacement. By allowing employees to bring, and use, their own devices, they can always have up-to-date technology without the company constantly incurring the costs for new models. For many, this practice has been extremely beneficial as many budgets are being cut and organizations are forced to trim spending.

BYOD shift costs from the company to the user and allows employees to use their own devices. BYOD policies also allow employees to use the technology that they are comfortable with and that they prefer, rather than what the company dictates they them. Users also may upgrade their devices to the newest features more frequently than what the company can afford to budget for on an ongoing basis.

Risks

Support of many different devices

Though there are many benefits to allowing BYOD, there are several risks that concern the IT staff. First of all, since it is not one standard device that everyone is using, the IT department will need to support many different types of devices and operating systems. This makes it very difficult to mitigate an issue with a device when the user needs assistance.

No control over what is on device

Organizations have no control over what types of applications are put on the device, which makes it very difficult to enforce security. Though employees probably would not download games or other entertainment applications on their work computer, in the case of BYOD, since the device is their own and also used for pleasure, they will certainly download numerous types of personal applications on the device.

Security Risks

BYOD increases the risk of having a security breach of important data. When an employee leaves the company, they do not have to give back the device, so company applications and other data may still be present on their device. This can lead to some company data being unsecure. There are also certain compliance regulations that businesses have to follow, such as HIPPA or GLBA, which are difficult to enforce when a device is not owned by the company.
Infrastructure Issues

Different types of devices operate at different speeds and with different operating systems. This can be difficult for an IT department to set up and maintain infrastructure to support different device needs. Also, if employees are able to bring their own devices, there will be many more devices used than what would be if the company was providing them. Employees might bring all of their phones, tablets and computers to work, meaning there will be much more strain on the company’s Wi-Fi and network.

Solutions

Easily setup new devices

With an influx of devices the IT department will need to add them all to the network, which can be extremely time consuming. Solutions such as Tools4ver’s User

Management Resource Administrator (UMRA) allow IT staff to easily add these new devices by adding them in Active Directory. End users will even be able to register their devices themselves if required.

Only allow certain devices to be registered

Since there are many different types and brands of devices that employees can use, an organization will have to decide which ones it is going to allow and support. This allows it to focus on a narrower selection of devices and be able to solve issues that arise with those devices. When a user tries to register a device, UMRA can be set up to only allow supported devices to be registered, thus not allowing unsupported devices to be registered on the company network.

Ensure Security

Security is a big issue with allowing BYOD at a company. When an employee leaves, he takes the device with him, so it is important that each departing employee does not still have access to important company data. With UMRA, once an employee leaves the company, his account can automatically be disabled, thereby deactivating his access to the network and any secure data. This ensures that when an employee leaves he will not be able to continue accessing important company data. This can also help to comply with regulations and audit needs. No one will have access to applications and data that they are not supposed to have access.

Dean Wiech is managing director at Tools4ever. Tools4ever supplies a variety of software products and integrated consultancy services involving identity management, such as user provisioning, role-based access control, password management, single sign on and access management, serving more than five million user accounts worldwide. For more information, visit their website at www.tools4ever.com *[1].*

Links:
[1] http://www.tools4ever.com