The discussion for this meeting revolved around allowing employees to bring and use their own devices, laptops, and desktops in the workplace. If these devices are allowed, how do they work with the support team?

**What are the member companies doing?**

Most of the companies agreed that their employees could and should bring their own cell phones to work and that they shouldn’t bring their laptops but disagreed as to devices such as iPads and other tablet devices.

At some of the companies a difficulty arises because some of the higher ups are very Apple focused while the company itself uses others including the Android and Microsoft software.

A few of the companies have a policy in place that excludes laptops but allows for phones and tablets. The policy also stipulates that the company can subject the device to a random audit and that it can be remotely wiped if it is lost or stolen. The employees are required to tell their employer if the device is lost or stolen. The companies with these policies also require that users have a key code set to protect the device if it is stolen.

No companies present blocked all forms of employees bringing their own devices. For some with contractors they are allowed to bring their own laptops to work but they must connect to a separate network and they are not allowed access to many of the systems.

One company has been working to provide a tablet to their employee that combines the functions of a laptop with the mobility of a tablet. Most of the companies agreed that using the tablets as is, was extremely difficult and it was better to make them function towards what the company specifically needs.

**What makes a laptop different from a cell phone or a tablet?**

One of the reasons discussed was that cell phones and tablets are used as consumption devices and not to create documents or presentation. These are devices that are easy to use in the field and mostly contain sales and meeting information rather than the proprietary information that may be stored on a laptop.

Another point raised is that phones and tablets are easy to run and difficult to break due to what they are used for. This cuts back on the need for the support teams to fix laptops because most of the problems with these devices correct themselves.

**How do you handle it if an employee’s personal device breaks?**

A question was posed as to whether or not the companies should keep loner devices on hand or provide service to the employee’s device if it breaks.

Most of the companies did not deal with this issue as far as actual device breakage because most people had office computers and did not have many phone or tablet issues. The biggest support desk issue for these companies dealt with the key codes and password resets as well as connectivity issues that mostly pertained to an older employee.

**What problems arise from allowing people to bring or use their own devices?**

Some of the problems that arise are the spread of viruses from outside devices to those that are within
BYOD to Workplace Friday, January 24, 2014

the network of the company. Even if the guest devices are on a separate VLAN they can still give the other devices on that VLAN whatever virus they have, purposefully or not. They may also not have access to the systems that they need such as printers etc.

It also brings up a security concern as to what information can be saved on these devices and what happens if the device is lost or stolen.

There may be liability issues if the employee does something with their device that they shouldn’t or if they lose proprietary information but most companies felt that the benefits of some of these devices far outweigh this liability and felt that the liability exists with or without the user bringing their own device.

Some of the companies discussed the cost associated with the implementation of BYOD because it would require the security to be moved to the network level and may even require some companies to create two different networks.

Another issue that was brought up was the issues that arise between exempt and non-exempt employees. If employees are allowed to work form home or their own device it may be difficult to track hours and overtime or to correctly allocate hours of actual work rather than simply being logged on.

Tax issues may also arise for employees working from home or from their own device. If a certain number of hours take place in another state or country then they must pay income tax to that state or country.

What about employees outside of the U.S.?

Some of the companies allowed employees of the their service desk to connect remotely and work from home. In some countries the VPNs are blocked and in some they cannot dial an U.S. 800 number, which makes remote access very difficult. The connectivity and infrastructure are also issues in other countries.

Another issue is that the cultural and communication differences are vast in many of the countries, which makes voice communication harder. Face-to-face communications, even virtual, is a benefit of allowing for remote connection and remote access.

What is the future of BYOD?

As companies move towards more cloud based applications and Office 365, employees are able to access their work documents via their own computers and networks.

Most of the companies present felt that they would not be allowing laptops in their companies anytime soon but did understand that as the number of devices available grow and change their policies will also have to grow and change.

http://www.gartner.com/technology/topics/1