

## BYOD IT Challenges

See Kay Leong (11 mins)

Let's look at what the IT folks really want in the company. On the surface, BYOD connectivity may look like a simple extension of enterprise mobile services, however, user expectations and the diversity of devices create unique infrastructure demands and challenges for IT operations to support mobility. With the growing adoption of BYOD, the workspace needs to cater to the demand for increased consumerization, mobilization, and virtualization, and all these require additional capabilities, and tools to further facilitate worker's productivity, ease of use, while adhering to company policies and security guidelines.

Let's look at the challenges and considerations from the company's perspectives.

### ***First, providing device choice and support.***

Traditionally, IT pre-determined a list of approved workplace devices, typically a standardized desktop, notebook, and maybe a small set of mobile phones or smartphones. Employees could choose among these devices, but generally were not allowed to deviate from the approved devices list.


With BYOD, IT must approach the problem differently. Devices are evolving so fast, that it is not practical to pre-approve each and every device brand and form-factor. It would be somewhat impractical to expect IT organizations to have the same level of support for each device that employees may bring in to the workplace. It would be a support nightmare.

Hence, most IT organizations have to establish what types of devices they will permit to access the network, they may or may not exclude a category or brand due to unacceptable security readiness and other factors that may impact the day-to-day support needs from the IT organisation.

### ***Second, On-Boarding of New Devices***

Other things to consider is to be able to adopt to a more IT-assisted and self-support model. Most BYOD implementations involve a wide-range of devices including desktop PCs, laptops, notebooks, smartphones, tablets, e-readers, and mobile collaboration devices. Some devices may be owned and managed by the company, while other devices may be employee purchased and self-supported.

On-boarding of new devices, which is bringing a new device into the network for the first time. Ideally, this should be simple and self-service, with minimal IT intervention,



especially for employee-bought devices. The IT team also needs the ability to push updates to on-boarded devices as required.

Ideally again, on-boarding should be clientless. What it means is that no pre-installed software is required. With this, it has an added benefit: if a self-service on-boarding model is successfully implemented, it can be easily extended to provide access to guests as well.

### ***Third, Maintaining Secure Access to the Corporate Network***

Maintaining Secure Access to the Corporate Network. We need to provide a flexible device choice, not having to sacrifice any security requirements. IT organisation must establish the minimum security baseline that any device must meet in order to access the corporate network, including Wi-Fi security, VPN access, and any software to protect against malware.

This is critical- to be able to identify each device connecting to the network authenticating both the device and the person that is using it.

### ***Fourth, Enforcing Company Usage Policies***


With this, we can then look at enforcing company usage policies. Most businesses have a range of policies that need to implement, depending upon their industry, regulations and the company's own policies. Adopting BYOD must provide a way to enforce these policies, which can be more challenging on consumer devices like tablets and smartphones.

Other complication results from the mixing of personal and work tasks on the same device. Most likely, employees will use their smartphones for both business and personal calls, while tablets likely to have personal data, personal and business applications installed. Accessing to the Internet, peer-to-peer file sharing, and application use may be subject to different policies when a user is on their personal time and network and when they are accessing the corporate network during work hours.

### ***Fifth, Visibility of Devices on the Network***

Traditionally an employee will have a single desktop PC and notebook or probably a desk phone. If the employee called IT for support, it would be straightforward to locate user's device on the network and troubleshoot the issue if necessary. Now, with BYOD, visibility of devices on the network is very key here.

Each employee is likely to have three, four, five, six..or even more devices connected to the network simultaneously. Many of the devices will have multiple modes, able to



transition from wired Ethernet to Wi-Fi, and as you move out of the office, roam to 3G or 4G mobile networks, moving in and out of these different connectivity modes during a session. It is critical for IT to have the tools that be able to see where you are, what you (are) doing. Basically, having visibility of all the devices on the corporate network and beyond.

### ***Sixth, Protecting Data and Loss Prevention***

Then, we look at protecting data and loss prevention. One of the biggest challenges with any BYOD implementation is to ensure the protection of corporate data. If a corporate asset, such as a laptop, is used to access business applications and data, typically that asset is tightly controlled by IT and likely to be restrictive in terms of the usage by policies.

Some industries need to comply with confidentiality regulations, example, HIPAA, which is Health Insurance Portability and Accountability Act in the US, or security compliance regulations like PCI-Payment Card Industry Data Security Standard, or in general, security practice regulations. Companies need to show that compliance is possible with BYOD adoption, which can be more challenging than a corporate-owned and managed device.

An employee-owned tablet or smartphone is likely to be used for personal access and business applications. Cloud-based file sharing and storage services such as Dropbox, Goggle Drive are convenient for personal data, but convenience always come with a potential sources of leakage for confidential corporate data.

It is very important for IT organization to have a strategy for protecting business data on all devices whether corporate managed or employee self-supported and managed. Some possible solutions are to have secure business partition on the devices, which acts as a container of corporate data that can be tightly controlled and may also include the need for a Virtual Desktop Infrastructure which in short, means VDI application to allow access to sensitive or confidential data without storing the data on the devices.

### ***Seventh, Revoking Access***

At the same time, in the lifecycle of a device or employee, it may become necessary to terminate access to the device. This could be due to the lost, stolen (device), employee termination, or even as simple as employee changing roles within the company.

IT organisation needs to be able to quickly revoke access granted to any devices and possibly wiping any of the data, that is not applicable for this user in his new role. For example, or as if he have left the company, then, on his personal devices, he should not have any access to such applications and data.

### ***Eighth, Potential for New Attack Vectors***

Now, again on security, because these devices access the corporate network, have wide-range capabilities and IT may not be able to fully evaluate, qualify, and approve each and every devices. Hence, the potential for new security attack vectors are opened.

For example, tablets have the capability to enable an ad hoc wireless LAN connection. If an authenticated device has other devices tethered to it through an ad hoc wireless LAN, it may be possible for the non-authenticated devices and users to gain access to the corporate network by connecting through the authenticated device. The same is true when tethering a laptop over Bluetooth through a smartphone.

The challenge for IT is how to permit the growing number of devices and capabilities to be used, while still maintaining the control to enforce policies, such as automatically disabling an ad hoc wireless LAN function on an authorized connected device.

### ***Ninth, Ensuring Wireless LAN Performance and Reliability***

As wireless access becomes pervasive, users may expect the same level of performance and reliability using wireless network as if (they) are using a wired network. This fundamental shift demands that IT change the service level of the corporate WLAN network from one of convenience to a mission critical business network, similar to that of a wired network. Design and operation of the wireless LAN must include high availability, performance monitoring and mitigation, most importantly, it's seamless roaming, from Wi-Fi to a wired network.

### ***Tenth, Managing the Increase in Connected Devices***

The increasing number of devices connected to the network, due to each employee having many devices simultaneously connected, can lead to IP address starvation as most legacy IP address plans were created under the assumption of fewer devices. Nobody has guessed (foreseen) this explosion of personal devices that has grown so much. This may hasten the need for a IPv6 deployment both at the Internet edge as well as inside the enterprise network.

### ***Eleventh, Work and Personal Overlap***

Work is an activity that people do, its not a place to which they go. Extended connectivity through mobile and remote access to the corporate network gives employees tremendous flexibility and increased productivity. It also leads to the blurring of line between work time and personal time, with employees trading set work schedules for the flexibility of working when and where they want to, often interweaving work and personal tasks.