Expert Reference Series of White Papers

Twelve Steps to Bring Your Own Device (BYOD) Success

Twelve Steps to Bring Your Own Device (BYOD) Success

Paul Simoneau, Global Knowledge Senior Instructor and Course Director

Introduction

Whether one calls it Consumerization or the Bring Your Own Device (BYOD) era, it has clearly begun in earnest. The availability of 4G (Fourth Generation) phones, tablets, hot spots, and other offerings, and their usage are expanding at amazing rates. Cisco's Visual Networking Index: Global Mobile Traffic Forecast Update 2011-2016 [1] provides some eye-opening statistics for 2011:

- Average Smartphone traffic was 150 MB per month, up from 55 MB in 2010.
- Smartphones are 12 percent of handsets, but they account for 82 percent of handset traffic.
- 4G connections generated an average of 28 times more traffic than non-4G.
- Smartphone average mobile network connection speed was 1344 kbps.
- Mobile-connected tablets tripled to 34 million.
- Tablets generated 3.4 times more traffic than the average smartphone.
- Each of 175 million mobile network laptops did 22 times the traffic of a smartphone.
- Mobile data traffic per laptop was 2.1 GB per month, up 46 percent.
- 33 percent of handset and tablet traffic was off-loaded onto the fixed network.
- Mobile video traffic exceeded 50 percent for the first time.

The same document projects that over the next five years:

- Over 100 million Smartphone users will be in the "gigabyte per month club" by 2012.
- Mobile-connected devices will exceed the world's population in 2012.
- Average mobile connection speed will surpass 1 Mbps in 2014.
- Smartphone handsets will exceed 50 percent of mobile data traffic in 2014.
- Monthly global mobile data traffic will surpass 10 exabytes in 2016.
- Mobile tablet traffic will surpass 1 exabyte per month in 2016.
- Tablets will exceed 10 percent of global mobile data traffic in 2016.

With that coming at an IT department, now is a good time to look at the challenges and opportunities of BYOD. Here are 12 areas that deserve careful consideration.

1. Security

Most enterprises considering BYOD think of security first. After that initial reaction, the importance of the details will quickly vary. For example, securing the mobile device is important for different reasons, such as:

- Preventing access to the enterprise network by an unauthorized user of an authorized device
- Preventing unauthorized access to sensitive enterprise data that may be stored on the mobile device
- Preventing any malware from infecting the mobile device and then the enterprise network
- Preventing unauthorized access to the user's personal information

For these and other reasons, consider the following steps:

- Establish a whole device password requirement with strong parameters such as at least eight characters, 90-day change rule, lockout after 5 failed attempts, etc.
- Specify that "jail-broken" devices are unacceptable for enterprise network access
- Secure the enterprise network independently from the mobile devices
- Protect the enterprise data by keeping it in the enterprise and displaying an image on mobile devices, possibly via Virtual Desktop Interface (VDI)
- Turn off Bluetooth
- Restrict ad-hoc networks to enterprise employees
- Create different access procedures for different user groups such as Guest, Executive, IT, Sales, Service, and Employee
- Implement same-day de-authorization on user's departure from the enterprise
- Monitor each authorized mobile device's communication with the enterprise, including user's authorized server(s), device location, and application(s) used
- Develop a rapid reporting procedure for lost or stolen devices
- Introduce the use of a Proxy Server for Guest access
- Require each user access enterprise networks using 3G/4G or Virtual Private Network (VPN) when away from enterprise network infrastructure

2. Inventory

Today's users often carry multiple mobile devices, such as a laptop, a notebook, a netbook, a tablet, and/or a Smartphone. A user will own some of those mobile devices. The enterprise will own the same make and model or similar mobile devices. Before granting access to the enterprise network, careful planning requires an inventory of the devices requesting network access.

Each mobile device has been on the market long enough to have seen multiple changes or upgrades to the operating system and other specifications. When adding devices to the enterprise network inventory, consider including the following items:

- User
- User e-mail
- User phone
- Device ID
- Make and model
- Operating System
- Firmware version
- Storage
- Wi-Fi versions supported
- Cellular access (3G, 4G, both)
- Carrier
- Wired access
- MAC address(es)
- Software applications

3. Registration

After adding the mobile devices to an inventory and deciding which of them are eligible to access the enterprise network, there must be a registration procedure. The enterprise IT department may choose to develop this software in-house, though most will find a it easier to use a Mobile Device Manager (MDM) package to support this process.

Since guests will have devices that missed the inventory portion, they will have a much shorter registration process and much more restricted access. Many organizations will require a signed Acceptable Use Policy (AUP), to grant them access to a designated wireless LAN (WLAN) and direct all traffic to a proxy server to limit access and bandwidth.

Using the inventory information and following steps in the procedure, the remaining users should be able to complete the tasks required to begin access. Those steps will include:

- Login
- Password
- Authentication code
- VPN setup

4. Estimates

There is a finite limit to the number of mobile devices and applications that any enterprise network can support. BYOD dramatically increases the strain on the enterprise network, and it is, therefore, paramount to analyze potential bandwidth needs and possible challenges.

Many tools for bandwidth analysis and estimating user traffic loads in a wired network will also support the same tasks on Wi-Fi resources connected to those wired networks. Beyond MDM solutions, protocol analyzers, Simple Network Management Protocol (SNMP)-based network management systems, and Java-based network monitoring offer the data and reporting solutions to make these estimates more accurate and help the IT department better plan.

5. Bandwidth

Controlling the amount of network bandwidth used by mobile devices works in much the same way as with wired devices; therefore, there are some choices to be made regarding how best to proceed for optimal bandwidth. The choices include using a proxy server for restricting access to certain websites that require more bandwidth such as social networking sites and video replay sites. Another alternative is to use router-based traffic shaping. Since mobile devices connect via Wi-Fi, enterprise infrastructure will need to expand in that area.

6. Tracking

Keeping track of mobile device uses and usage improves the accuracy of traffic estimates as well as bandwidth planning. With the tools already in use above, enterprise IT staff will be able to track the activity of individuals, groups of users, applications, classes of applications, and also provide security input similar to Intrusion Detection Systems (IDS).

Knowing where mobile users are going and what they are doing in the enterprise network makes proactive network troubleshooting, network planning, and infrastructure adjustment more accurate and effective.

7. Compliance

Many of the regulations relating to enterprise computing and networking came into effect before the rush of mobile devices occurred. The challenges are to follow those regulations without having control over all the BYOD communications. For example, complying with the Public Company Accounting Reform and Investor Protection Act or Sarbanes-Oxley Act's [2] retention of e-mail and instant messages leaves out the cellular Short Message Service (SMS) and the potential that social media engines such as Twitter brings.

Separately, some states and countries (such as the UK's Data Protection Act [3]) require written notification to users that you are monitoring their online activities and why. Adding this notification to the AUP that the user signs before accessing the enterprise network is just one more way to help maintain compliance.

8. Storage

In the best of all worlds, the expanded storage on a mobile device would be clear of any enterprise data, or sensitive or public knowledge. It is in the users' best interest to be sure this is true. Many enterprise IT departments are requiring a "force wipe" program to remove any enterprise data from the users' mobile devices upon an employee leaving the enterprise or when the device is lost or stolen. This program may also wipe all personal data.

By using VDI, the enterprise keeps its data securely on its data center drives and only shows a copy to the user. A true VDI will compliment the security controls addressed in the security section above.

9. Financial

When an enterprise decides to allow BYOD access, some financial questions are bound to arise. Is this mobile device access a business cost or a convenience to the user? Will this apply to all employees or only a select

group? Does the enterprise compensate the user for purchase, for monthly carrier charges, for insurance, for replacement…? How does the enterprise decide?

Most organizations have decided that the mobile device is an acceptable business expense. Those who have made that decision have also specified who in the enterprise will qualify, based on their job description. Those who qualify will receive a compensation based on business need. Stipends for purchases have a set limit, must be returned if the user leaves within a given time frame, and may only be used on a set periodic basis such as once every two years.

10. Multiples

More and more users will own two or three mobile devices that will be used in the enterprise. Unlike single-location desktop computers, these mobile devices may access the enterprise network simultaneously. For example, while online in a conference call or webinar, a tablet could be useful in looking up supporting facts as a Smartphone checks for and responds to messages. Accurate and complete tracking and logging of each device supports security, network monitoring, and network traffic flow.

11. Ownership

While most organizations have left mobile device ownership to the users, some have taken other routes. A few have purchased the devices for a minimal fee so that they may have legal control of the device and then resell it to the user at a future date for the same minimal amount.

Many BYOD enterprise solutions involve organization-owned mobile devices. These may be loaned to certain designated users instead of the users buying their own device. It is also a good idea to have spares ready to loan to users whose mobile device is damaged, stolen, or lost so that they may continue their work while a replacement is purchased, configured, inventoried, and registered with the network.

12. Revocation

There will come a time that the mobile device (or the user) will need to have access revoked. In the case of the user, it could come from an AUP violation or departure from the enterprise or changing jobs in the organization. With the monitoring, tracking, and logging of each device, it is much easier to know if data may be stored on the device and to what extent so a limited wipe of enterprise data and configurations may be all that is required before user departure.

With the mobile device, there could be major damage, or it may have been stolen, or even just lost. A full remote wipe of the device, with confirmation, is the best solution, and it should happen as soon as it can be done.

Conclusion

IT departments have multiple opportunities and challenges as a result of the BYOD invasion. The most common opportunity is to reinforce enterprise network security from both the inside and the outside. Supporting BYOD

also offers more monitoring and tracking of activities that provides a more detailed view of network traffic flow. Beyond that, IT will gain valuable insight into which devices work best with the layout of the enterprise network. Lastly, hardware cost savings can be realized by IT departments since employees will have purchased their devices enabling IT to maximize funding to update and strengthen the infrastructure.

Alternatively, it will be a challenge for some IT departments to give up control over which devices may access their enterprise network. Another challenge will be to have the users doing configurations for network access which adds human error to a crucial part of the process. As a result, that may increase the number and frequency of calls to the help desk. IT can turn that into an opportunity by creating a mobile app to streamline and control the registration process.

The opportunities and challenges BYOD represents are real. Enterprises must make their network infrastructure BYOD-ready to meet the onslaught.

Footnotes

1 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

2 http://www.techrepublic.com/article/what-the-sarbanes-oxley-act-means-for-it-managers/5034345

3 http://www.mofo.com/monitoring-employees-striking-a-balance-10-22-2007/

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, check out the following Global Knowledge courses:

Understanding Networking Fundamentals

TCP/IP Networking

Troubleshooting TCP/IP Networks with Wireshark

Network Management: Tools, Optimization, and Troubleshooting

Practical Techniques for Analyzing Wi-Fi Traffic

iPad Support Essentials

Security+ Prep Course (SYO-301)

VMware vSphere: Install, Configure, Manage [v5.0]

VMware View: Install, Configure, Manage [v5.0]

Cloud Computing Essentials

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Paul Simoneau has well over 35 years of experience in working with multiple aspects of computers and data communications. He is the founder and president of NeuroLink, Ltd., an international coaching and education company specializing in professional development. NeuroLink's client list includes Cisco, AT&T, Apple, Lucent, Citibank, Visa, GE, Quest Communications, Hewlett-Packard, Sprint, Verizon, US House of Representatives, US Senate, Many departments of the US government, including all branches of the US Armed Forces, and many others.

He is a senior instructor and course director with Global Knowledge, the blended solutions training company. His writing is also recognized outside of Global Knowledge in the *Hands-On TCP/IP* and *SNMP Network Management* books published by McGraw-Hill.

A graduate of the State University of New York at Albany, he also holds a Masters Degree from Webster University.