Fifteen Steps to Conquering BYOD

By Gary Audin, Angela Wyant, Wayne Shumate

April 26, 2012

Bring Your Own Device (BYOD) is not a single product, not a single service, not a single application. It is a situation where IT does not own or distribute the endpoints. It is a user driven phenomenon that IT MUST eventually embrace and then learn to manage BYOD and surmount the challenges. The enterprise has to gain control of BYOD or risk business anarchy that affects the enterprise's productivity, security, privacy, regulatory compliance issues and reputation.

- **Challenge # 1 –** The enterprise is not the device owner and nor is it the wireless service provider subscriber.
- **Challenge # 2 –** IT is responding to the rapid BYOD growth, usually not initiating it.
- **Challenge # 3 –** The user may have more than one device in use.
- **Challenge # 4 –** There may be information overlap, multiple applications in use and the need to ensure application accessibility.
- **Challenge # 5 –** Data protection is required, but is complicated by the BYOD user communicating with non-enterprise social networks.
- **Challenge # 6 –** The user expects to use multimedia.
- **Challenge # 7 –** Ensuring that the existing infrastructure can support BYOD access and traffic.
- **Challenge # 8 –** Developing, implementing, and enforcing new access and usage policies, covering both the device and the user's role in the enterprise.
- **Challenge # 9 –** Training the help desk and trying to avoid overload.

Creating BYOD policy and enforcing it can be a headache for IT.There are no right or wrong policies or procedures. Each enterprise must develop its own decisions based on the business benefits, technology requirements, regulatory, security and privacy issues, and employee expectations and benefits. There are 15 recommendations at the end of this paper for the enterprise to implement an effective BYOD plan and policy.

[1] *Originally posted at www.nojitter.com under the title "Plan for – Don't Inherit – BYOD"*

BYOD IS INEVITABLE

The IDC survey “2011 Consumerization of IT Study: Closing the Consumerization Gap,” IDC Survey, sponsored by Unisys, July 2011 asked IT executives to rate their level of agreement with employees’ use of personal devices. These executives recognized that employees’ use of BYOD is going to happen, will increase morale, improve productivity, and be essential to business objectives and services. IDC also did state BYOD will increase workload for IT and help desk staff. The survey results are that:

- 69% thought tablets, iPads and other like devices will be part of the business tools used.
- Unfortunately, 57% thought that IT will have an increased workload when these devices come into use.
- 52% of executives expect that their devices need to be supported.
- 43% thought that a BYOD policy would increase morale.
- 37% thought a BYOD policy would improve productivity.

MANY DEVICES, MANY OPERATING SYSTEMS

The graphic below, is based on “Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent,” showing the worldwide market share for mobile devices and smartphone operating systems. There are many smartphones and operating systems available, that IT organizations will find it challenging to support any and every device an employee might use.

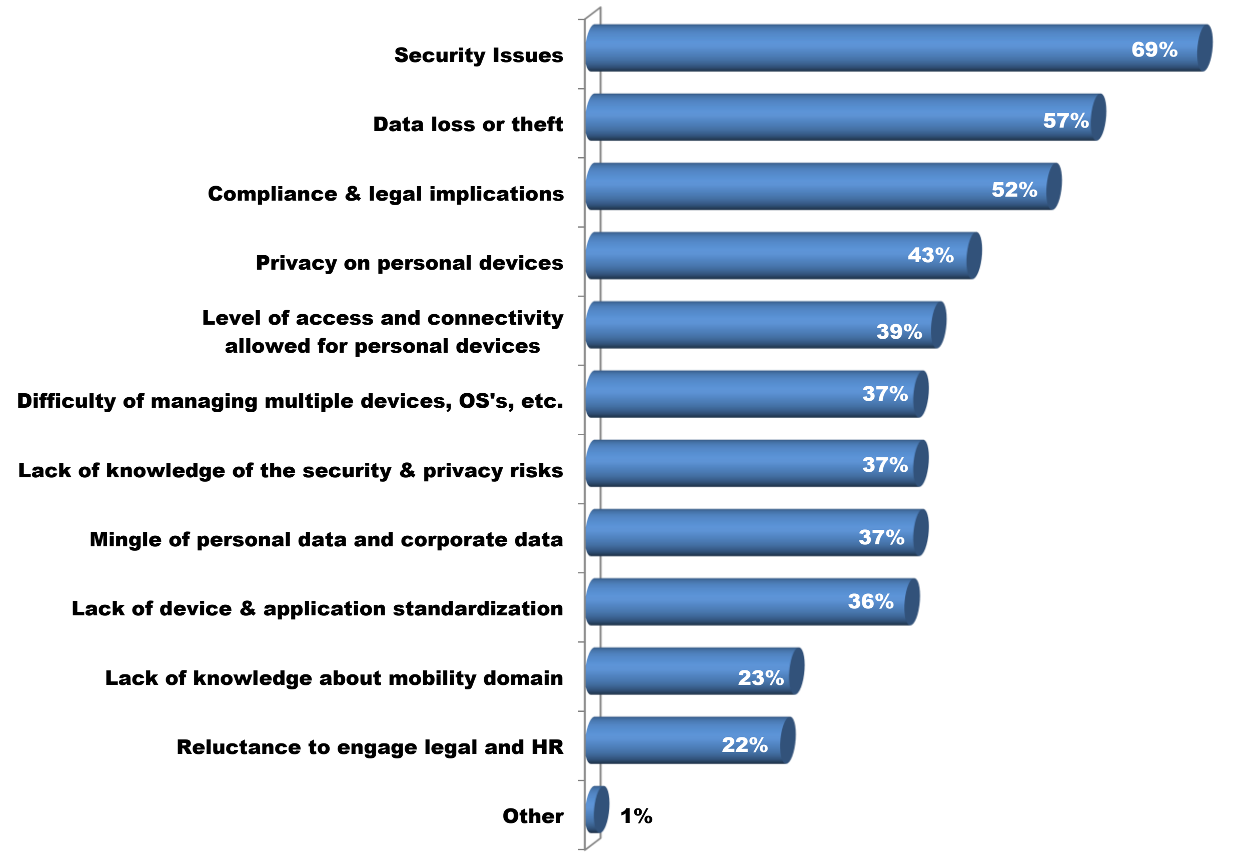
Some analysts focus on the BYOD device. What is more important is the operating systems in use. When applications and security software is implemented in the device, the operating system is what matters. One of the impacts on the enterprise is the fact that at least five operating systems will need to be supported, Android, Symbian, iOS, RIM and Microsoft.

According to a Gartner press release, “Gartner Says Sales of Mobile Devices Grew 5.6 Percent in Third Quarter of 2011; Smartphone Sales Increased 42 Percent”, the operating system use balance is changing as of 3Q11. Android device sales increased sharply from 3Q10 to 3Q11. Symbian based device sales as a percentage of sales were cut by over 1/2. iOS sales decreased slightly and RIM sales were reduced about 1/3. Microsoft is a distant fifth in the mobile OS market. This makes it even harder for the enterprise because the operating system mix is not constant. Although with all the sales change the top five operating systems to support remains the same.

KNOW THE RISKS

The Trend Micro survey results, “Enterprise IT Consumerization Survey June 2011,” Trend Micro, June 2011 shown below lists concerns IT staff have identified for employees’ use of personal devices in the workplace. These concerns provide a broad overview of some of the risks faced. They can be used to inform executive staff of the issues that need to be investigated and mitigated in order to allow employees to use their personal devices to access the enterprise network and data resources

Concerns with Employee Personal Devices in the Workplace



Source: Trend Micro, June 2011.

DEVELOPING THE BYOD POLICY

It is interesting to note that almost all organizations allow employees to use mobile devices for business purposes. However, just over 50% of enterprises have indicated they had revised their cell phone policies to include employee-owned devices.

For those enterprises that have already started the transition to employee-owned devices, the following “pain points” can be identified:

- A clear, approved definition of enterprise-owned vs. employee-owned is necessary.
- Better staff communications are needed to describe the change to a BYOD policy.
- The length of time it took to get the policy in place can be longer than expected.

- The effort needed to work with carriers to keep the same phone number and features for employee-owned devices.

CREATING BYOD STANDARDS

Standards are important for all mobile devices, whether enterprise-owned or employee-owned. Almost all organizations have standards for mobile devices. While these devices are mainly enterprise-owned, it is critical for enterprises to develop and publish standards for employee-owned devices, operating systems, and levels of support. Most enterprises do not treat tablets and iPads differently than smartphones.

SUPPORT

Support for employees using mobile devices has become essential. This support may either be provided by in-house IT staff or through a 3rd party vendor. The vast majority of enterprises provide support for their enterprise-owned devices. A minority allow employees using personal devices to contact their Help Desk or IT department. As enterprises move to more employee-owned, they will have to review and evaluate their support procedures and communicate them appropriately to all users.

The use of a Mobile Device Management (MDM) Solution will help enterprises to effectively provision, deploy, and manage multi-platforms. It will be especially needed for enterprises that manage large numbers of mobile devices.

RECOMMENDATIONS

When the enterprise decides to move to an employee-owned mobility model, it is suggested the enterprise considers the following recommendations. These recommendations are based on an assessment of private survey responses, phone interviews, industry research, and telecomm experience by www.AHFCommunications.com.

1. **Establish a Mobility Committee**
   The Mobility Committee should include key executives, IT and user departments. The Committee will evaluate the benefits and risks of mobility options, develop the corporate mobility policy, set strategic goals, establish actions plans, and determine measures for success. The Committee will also need to clearly define "mobile devices” and identify all devices (e.g., smartphones, standard cell phones, iPads and tablets, aircards, laptops, PDA’s, USB’s, cars, cameras, etc.) that should be included in the policy.

2. **Determine the Current Mobility Environment**
   A mobility survey of employees and department managers should be conducted to provide a broader understanding of the business value and needs of the mobile workforce, define current usage, and provide knowledge of additional benefits not yet identified. IT should evaluate the mobility needs for employees in order to provide a competitive edge and maximize employee retention and morale. IT needs to know their current carriers’ contract terms to ensure they maintain commitments until contracts are open for revision. This carrier detail and usage data will help the transition from the corporate plan to an employee’s personal plan.

3. **Revise the Existing Cell Phone Policy**
   The current cell phone policy will probably be revised to include all current and future mobile devices, and policies and processes for employee-owned devices. This policy must address privacy issues and ramifications for noncompliance of corporate policies, and should be reviewed on an annual basis, especially since the mobile devices world is changing so rapidly. Employees should be informed that while connecting to the enterprise data and applications, their personal information such as SMS, MMS, e-mail and phone records are all available to the corporate environment. Employees must be made aware of the impact on their personal data if they lose their devices and/or the IT needs to wipe the device or data. Employees should be reminded that it is their responsibility to back up their own personal data.

4. **Accommodate Users While Protecting the Enterprise Network and Data**
   Moving to employee-owned devices shows that the enterprise is attempting to meet the needs and expectations of an ever growing number of employees who want to carry only one device, and have access to their enterprise e-mail, calendar, business applications, etc. Employees need to know IT will try as best as possible to accommodate their desire to use personal devices, but must, at all costs, protect the enterprise network and data. IT should manage mobile devices with access to information resources like they do PC's, and implement similar security, authentication, and protection procedures. IT should separate enterprise data from personal data.

5. **Ensure Compliance Regulations Are Followed**
   Privacy and regulatory decisions must be identified and evaluated for employee-owned devices. For example, will users with their own personal devices be allowed to use camera capabilities while at work? Are there any special regulations or compliance issues that apply? In addition, legal liabilities for employees' use of cell phones while driving or IRS changes in regulations for enterprise-owned cell phones must also be considered. IT should consult their legal department for guidance on what actions to pursue if illegal activity is discovered in the process of auditing an employee's personal device and records.

6. **Require Employees to Sign a User Policy Statement**
   All employees, especially those using personal devices, must be required to acknowledge and sign the user policy and procedures before obtaining access to enterprise resources. If an employee does not agree to all terms in the policy, IT must not allow the employee and device to access the enterprise network and data.

7. **Centralize the Management of Services**
   Centralized management of telecom services and support, to include cellular, mobile, and wireless technologies, provides the best organizational structure to control costs and continue to maintain an environment where mobility can grow while ensuring access to corporate data. Centralizing management provides the focused ownership needed to review polices, network security, job functions, and user requirements as mobile hardware and applications become available. In addition, it is important to continue to manage all associated telecom expenses, even when moving to employee-owned devices.

8. **Strengthen the Existing Security Policy**
Enterprises should evaluate and probably modify their current security policy and procedures to reflect the risks of employee owned devices. Employee owned devices should be secured with strong passwords and data encryption, and policies enforced that prevent data security breaches. Be sure users with employee-owned devices know that, depending on security, legal, or administrative needs, their devices may be wiped remotely. While every effort should be made to protect personal data on employee-owned devices, users should know there are no guarantees. IT security policies, procedures, and support applications should be evaluated and updated on a regular basis.

9. **Develop Corporate Standards for Devices and Platforms**
With an explosion of smartphones, tablets and even devices integrated in cars, it is critical to standardize on the type of employee owned devices, platforms, and operating systems that will be allowed and supported. This is especially true when IT is supporting these with in-house staff and applications. Where appropriate, the enterprise should utilize their existing Mobile Device Management (MDM) solutions that provide full life-cycle support for multi-platform devices.

10. **Create User Groups and Policy Standards**
Define and identify which employees, by user group, will be eligible for either enterprise owned or employee owned devices, the type of devices, applications and data allowed, appropriate stipend or reimbursement options, and levels of technical and help desk support. Define what users, devices, and applications will be fully supported by the organization, or perhaps not supported at all. If necessary, review and modify job descriptions, roles, and responsibilities.

11. **Determine Payment Options**
For each defined employee user group, identify how IT will fund employee-owned devices, whether by stipend, reimbursement, or not at all. These payment options should include voice and data services costs. Organizations vary on their approach to funding employee owned devices and there is no magic answer to this dilemma. Many organizations surveyed established the amount from their previous corporate plans. Stipends are recommended if expense reduction is the goal. Simple reimbursements limit any control on costs, especially if personal mobile plans are not negotiated appropriately by the employee, and, therefore, are not recommended.

12. **Minimize the Impact on IT and Help Desk Staff**
Trying to meet the needs and complexities of many different employee-owned devices and platforms will be very difficult for in-house IT and Help Desk staff. Adding to this challenge is the constant introduction of new smartphones and tablets into the marketplace, certainly at a much greater rate than traditional desktop computers and laptops. Consequently, an already over-burdened IT support staff will be asked to do more. To help reduce the number of help desk calls and IT support, a self-service portal could be setup or web resources utilized. Where appropriate, IT should utilize their existing Mobile Device Management solutions that provide comprehensive user support services. The ultimate objective is to improve employee satisfaction, productivity, and support.

13. **Develop a Communications and Training Plan**
IT must develop and publish a comprehensive communications and training plan to make sure all affected employees are aware of the new policy, standards, guidelines, and procedures. This plan should be published on a self-service portal or through web resources. In addition, it is important for employees to know the consequences of non-compliance with the new policy. Portals and training resources should be updated on a regular basis as applications, devices, and policies change.

14. **Evaluate Mobile Device Management (MDM) Solutions**
IT should fully utilize the features and capabilities of their existing Mobile Device Management solutions before moving to employee owned devices. These tools provide an organized approach to implementation, and can manage both corporate-owned and employee owned devices. Given the significant number of current and possible future devices, IT will be required to manage and use a MDM solution which will be essential for successful provisioning and deployment, device and application security, and user support.

15. **Measure the Results**
A critical component of a move to employee owned devices is to measure the results to show that initial goals and objectives have been achieved. Key metrics would include dollars saved, employee satisfaction, and help desk response time.

Implications for the Enterprise

With respect to the industry insights, information, and figures shown above, IT should:

- Study the impact of employee owned devices on its staff in order to provide a high level of service and support for users and devices.

- Standardize on mobile platforms and, more important, use their existing Mobile Device Management Solutions to manage the possible multi-platforms.

- Identify and evaluate all risks associated with employees' use of personal devices to include network, data, security, privacy, business, compliance, and legal.

About Gary Audin

Gary Audin Delphi-inc@att.net has more than 40 years of computer, communications and security consulting and implementation experience. He has planned designed, specified, implemented and operated data, LAN and telephone networks. These have included local area, national and international networks as well as VoIP and IP convergent networks in the U.S., Canada, Europe, Australia, Caribbean and Asia. He has advised domestic and international venture capital and investment bankers in communications, VoIP, and microprocessor technologies.

Gary Audin's many articles can be found on www.webtorials.com, www.telecomreseller.com and www.acuta.org. He writes a weekly blog on communications subjects that can be found at www.nojitter.com and publishes technical tips at www.SearchTelecom.com, www.SearchNetworks.com and www.SearchUnifiedCommunications.com.

Gary Audin's co-authors are Angela Wyantis, founder and President of AHF Communications, a vendor neutral consulting firm in Charlotte, NC; and Wayne Shumate, Senior Consultant for AHF Communications.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

This report was prepared by Gary Audin of Delphi, Inc., and edited by Steven Taylor, Co-founder, and Leslie Barteaux, Senior Analyst / Editor of Webtorials.

Published by Webtorials
Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
Jim@webtorials.com
Steven Taylor
Taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.