2013

BYOD: Moving toward a More Mobile and Productive Workforce

D. Lance Revenaugh, Ph.D.
Montana Tech of the University of Montana

Michael E. Schweigert
Montana Tech of the University of Montana

BYOD: Moving toward a More Mobile and Productive Workforce

D. Lance Revenaugh
Michael Schweigert

Contact author:

D. Lance Revenaugh, PhD
Business and Information Technology Department
Montana Tech University
1300 West Park Street
Butte, MT USA 59701
Phone: (406)496-4411
LRevenaugh@mtech.edu

Michael E. Schweigert
Business and Information Technology Department
Montana Tech University
1300 West Park Street
Butte, MT USA 59701
Phone: (406)696-8816
MESchweigert@mtech.edu

Topic area: Business, Information Technology

Abstract

In recent years there has been a personal and organizational trend toward mobility and the use of mobile technologies such as laptops, mobile phones and tablets. With this proliferation of devices, the desire to combine as many functions as possible into one device has also arisen. This concept is commonly called convergence. Generally, device convergence has been segmented between devices for work and devices for home use. Recently, however, the concept of Bring Your Own Device (BYOD) has emerged as organizations attempt to bridge the work/home divide in hopes of increasing employee productivity and reducing corporate technology costs. This paper examines BYOD projects at IBM, Cisco, Citrix, and Intel and then integrates this analysis with current literature to develop and present a BYOD Implementation Success model.

Keywords: Bring Your Own Device (BYOD), Data/Device/IT convergence, IT infrastructure, Mobile computing

Introduction

As long as organizations have been around, they have been trying to improve their business processes. Within the last few decades, the personal computer boom changed how organizations operate and each business was faced with new challenges. Both becoming more efficient as well as saving organizational costs in IT.

One of the early attempts at decreasing IT costs was through the telecommuting. Since the creation of telecommuting, organizations have been finding new and innovative ways to reduce costs further while making their workers more productive. BYOD (Bring Your Own Device) is the latest innovation in IT that allows employees to use their own personal devices for work activities. This concept applies to devices such as smartphones, tablets, and laptops.

BYOD was created to limit the number of devices that each employee needed to carry and to take advantage of potential cost reductions in IT. Instead of carrying business and personal phones, an organization's IT staff can now converge both worlds into one simple solution through the use of BYOD. BYOD does present some new challenges, however, particularly with security and support becoming major factors. These and other factors that each organization needs to address before adopting a BYOD program will be examined.

Increasingly Mobile Workforce

Within the last two decades, the IT industry has had many advances in mobile technology. This has included a rise in more mobile devices such as tablets and smartphones (see Figure 1), and these devices have greatly complimented the already established thin client and laptop computers that businesses have used in their workforce. With these additional technologies, there has been an increase in the potential to expand data availability and the mobility of employees, thereby leading to at least the potential of greater productivity and profitability.

Figure 1: Common Mobile Devices

As many of these mobile technologies have become more available to the general public at a relatively low cost, the reality of employees carrying both office and personal devices has proliferated. While it may seem like a good idea to segregate personal and business devices, organizations have now realized they run an increased risk of their employees sending data back and forth between their work and personal devices. The advent of cloud computing and storage has further supported this trend. All of this has led to organizations re-examining IT convergence as it relates to corporate data security and employee productivity.

Device and IT Convergence

Many organizations are working toward gaining a competitive edge in their industry by seeking out more efficient business processes. Data convergence has become part of this effort as firms have sought to reduce data access points and data redundancy. A key benefit of the data convergence efforts has been that employees have more access to valuable network resources with more ease. With this data convergence, organizations are now starting to harness the popularity of technology or device convergence. Technology convergence is the concept of two similar technologies being combined to become more efficient. A few examples of this are a PDA and cell phone being merged into a smartphone, and printers, scanners, and copiers being merged into one multi-function device.

When IT convergence is embraced by an organization, networked applications are readily available and can be used to access data from any device that has the right permissions. Device convergence, complimented by virtualization of desktop environments, provides a more mobile workspace that positively impacts an employee's efficiency and effectiveness. However, when device convergence includes both personal devices and business devices, security and logistical issues becomes more complicated. In addition, some of the benefits of IT convergence can take years to fully develop and come to fruition. As an example, the current level of personal and business device convergence that we see today started informally as some firms began to allow only a few select executives to use their mobile devices for accessing corporate data. It took several years before some of these capabilities were extended to portions of the rest of the organization.

The Rise of BYOD

As the various aspects of IT convergence continued to evolve, organizations began to allow employees to use their personal smart phones to keep track of their professional contacts. As this business use of an employee's device grew in popularity, the concept of BYOD emerged. BYOD is an attempt to merge personal use and business use mobile devices into one. To complement the convenience of having one smartphone for both work and personal use, the concept has then expanded into tablets and laptops.

When many people think of BYOD, they only picture being able to bring their smartphones and tablets to work. As shown in Figure 2 below, that is just the beginning of the possible organizational benefits. When the majority of employees think of BYOD, they consider only the Simple Approach on the top section of the figure below. However, as shown, there is a much more vast Comprehensive Approach for organizations to consider. On the organizational end of BYOD, there are many positive factors to consider; increased agility, higher productivity and risk mitigation to name a few (Cisco Public, 2013).

Even with these potential benefits, however, BYOD has remained an informal practice in many organizations. The future appears to be different though, as large organizations in particular are seeing the need to change to a formal BYOD program (Citrix Systems, 2013; Cisco

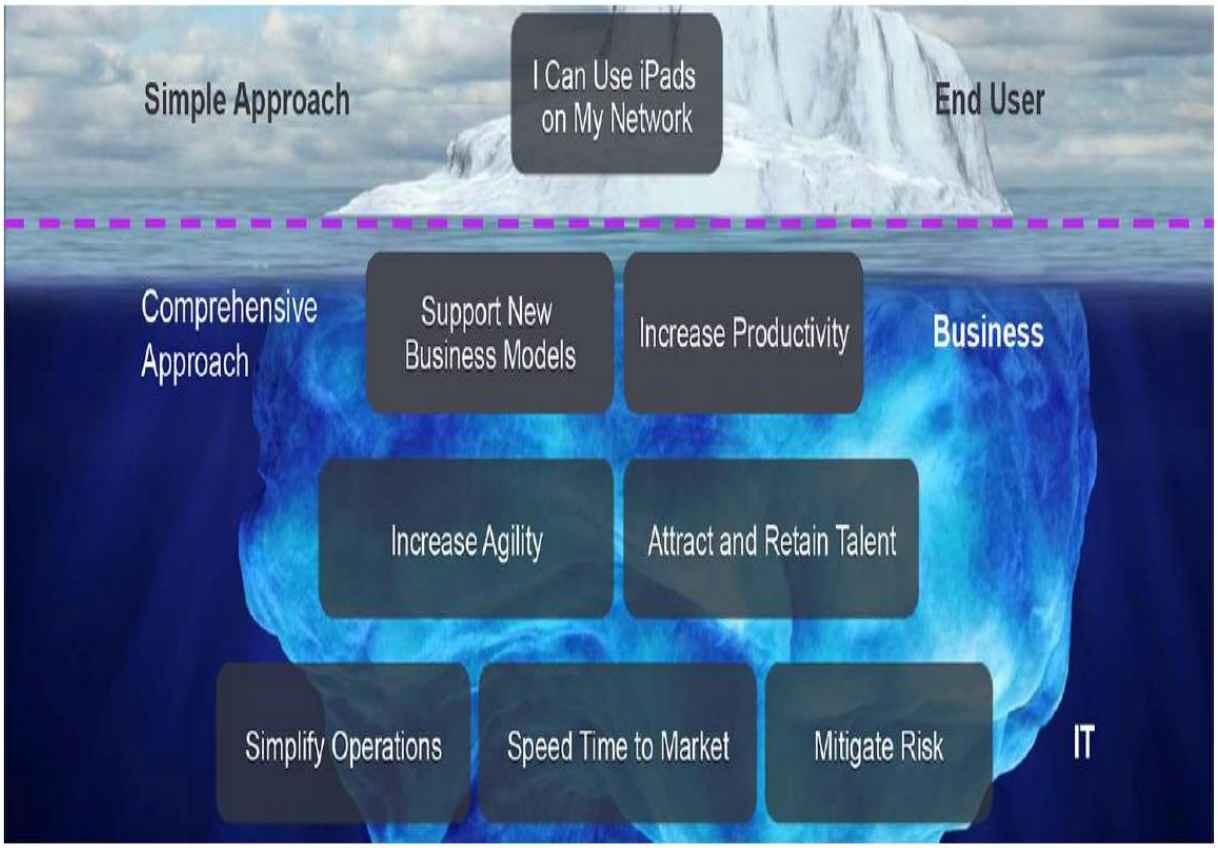

Figure 2: Comprehensive Approach to BYOD (Cisco Public, 2013)

Public, 2013). Through the use of a formal BYOD program, there is potential for the support of new and improved business models as well as simplified operations. On an individual basis, the increased availability of data with a BYOD policy, enabled each user to have increased agility during their workday.

Through implementation of a BYOD policy, organizations that were involved in pilot programs have successfully created the "always on" employee. By having an employee that always has their work with them, these organizations have created the potential for each employee to increase overall productivity. BYOD also enables employees to do their menial tasks in their free time rather than doing them when they should be working on a major project at the office. With the ability to work at unconventional times when the office would normally be closed, there is potential for more to be accomplished by the employee even after the organization has closed down for the day.

While BYOD has many benefits, it also presents many challenges and organizations have many factors to consider before implementing a BYOD program.

Implementations of BYOD

As stated earlier, many larger organizations are moving to a formal BYOD program. Cisco, Citrix, IBM, and Intel are organizations that have implemented their own BYOD policies with some success. Here we will discuss their experiences and analyze the BYOD adoption process. In the figure 3 shown below, the experiences and policies of these case study companies have been organized into five major categories.

The data in figure 3 reveals many potential challenges when an organization decides to develop and implement a BYOD policy. The case study organizations have shown, however, that with proper planning, the project can run smoothly and successfully. Though each of the organizations approached some of these issues differently, their experiences have been boiled down into the following five major categories:

- Security
- Mobile Device Management (MDM)
- Device Selection
- Training
- Support

Security

Security was each organization's highest priority. Depending on the type of organization, they needed to ensure that they were legally compliant with organizational standards. There are many different aspects of IT security to consider such as data, network and application security policies, as well as a specific mobile security policy. Each of these security aspects were considered up front before any implementation was started (IBM Global Technology Services, 2012.) To ensure the highest and most efficient form of security, it was recommended by both Intel and Citrix that access to any organizational resources be set on a user level with both access management and an integrated infrastructure (Buchholz, 2012; Citrix Systems, 2013). By restricting resources on a user level, IT staff is able to further monitor who is accessing the organizational data and restrict them based on their job.

	Cisco	Citrix	IBM	Intel
Security	-Identity based Policy Management	-Different levels of eligibility -Ensure compliance with standards	-Mobile Security Policy -Network and Application specific policies	4 Pillars • Business Intelligence • Access Management • Integrated Infrastructure • Data Protection
MDM	-MDM is critical -Complimented by Mobile Application Management Software	-Organization specific App store -MDM is vital to ensure mobile security	-MDM vital to organization security policy	-MDM critical for support and security -Handles configuration of devices
Device Selection	-Organizational Preference	-Organizational Preference -Set minimum requirements	-Limit number of platforms	-Limit number of platforms
Training	-Cisco Partners Provide Organizational Training	-Minimal, defined by IT staff -Data Separation	-Minimal, defined by IT staff	Essential, with 3 Levels • End User • Helpdesk Support • Developer
Support	-Cisco Partners -Internal IT staff	-Higher IT support expectations -Loaner Devices if lost or damaged	-Ongoing break fix support -Consider a mobile partner for additional support	-Internal IT support -Loaner devices if the original is lost/stolen/broken

Figure 3: BYOD Implementation Analysis

Mobile Device Management

Mobile Device Management (MDM) software is also at the heart of any BYOD program. MDM has allowed IT to enforce any security policies that have been written, as well as assist in the support of end users. MDM allowed the case study organizations to more easily deploy and distribute approved mobile applications based on organizational security policies. Proper use of MDM software also prevents data theft through unapproved apps, adds encryption for additional mobile threat management, and even allow administrators to remotely wipe a device in the event

of it being lost or stolen (IBM Global Technology Systems, 2012). While there are MDMs with the potential to manage applications, it is recommended by Citrix that each organization have its' own app store for easier management of applications (Citrix Systems, 2013).

Device Selection

When it comes to device selection, the standard policy of each organization is that less is more. The fewer platforms an IT staff or third party consultant needs to support, the higher quality the support will be. In terms of employee satisfaction, however, employees want to have more choices. Each organization has to figure out which of the different Operating Systems it wants to support. Each organization will have their own preferences for platforms and have a set of minimum requirements in place for each type of device. While allowing all device platforms isn't practical, it is certainly practical to support a specific line of devices, due to minimal changes in the OS. This has been realized by each of the case study organizations. In an effort to ensure high employee satisfaction, IBM created a team to administer a poll among employees to determine the most popular devices and platforms (IBM Global Technology Systems, 2012). While device selection was a priority for all BYOD organizations, Citrix also emphasized there are infrastructure considerations that must be addressed before determining which types of platforms to support (Citrix Systems, 2013).

Training

As expected with the new BYOD implementations, there were many calls to the support line. Proper training of employees, however, was undertaken in order to minimize support calls to staff. This was a priority particularly for Intel (Buchholz, 2012). Within the training program, Intel used multiple levels of training for employees: end user , helpdesk, and developer training and support. For the end user, the training included common issues, the best way to use apps, and proper organizational procedures. As for support staff, they were trained to navigate through the "back end" aspects of the devices in order to ensure that they could resolve any user issues. With development training, developers were trained in best practices when it comes to developing apps and features for the organization's mobile devices (Buchholz, 2012). Employees properly trained in business practices and applications can maximize the success of the BYOD implementation. Lastly, it has been recommended by Cisco and IBM that training be conducted by a third party professional, whether that training is done by a mobile partner or sister organization (Cisco Public 2013; IBM Global Technology Systems).

Support

Support came in many different forms. The majority of these organizations preferred having their own internal IT staff supporting their internal customer's mobile devices. Other forms of support that were used were mailing lists, web ports, wikis and other forum based websites that allowed end users to collaborate on common issues. This reduced the strain on support IT staff and resolved minor issues more quickly.

The BYOD Success Model

Combining foundational principles of organizational change and project management with the findings from the previous section, the BYOD Success Model was developed and is presented here. The model, as shown in figure 4, reveals that the key to any successful BYOD policy is not only the five categories that have been previously discussed, but also the ease of use of the policy as well as employee support. If the BYOD devices are not easy to use or don't

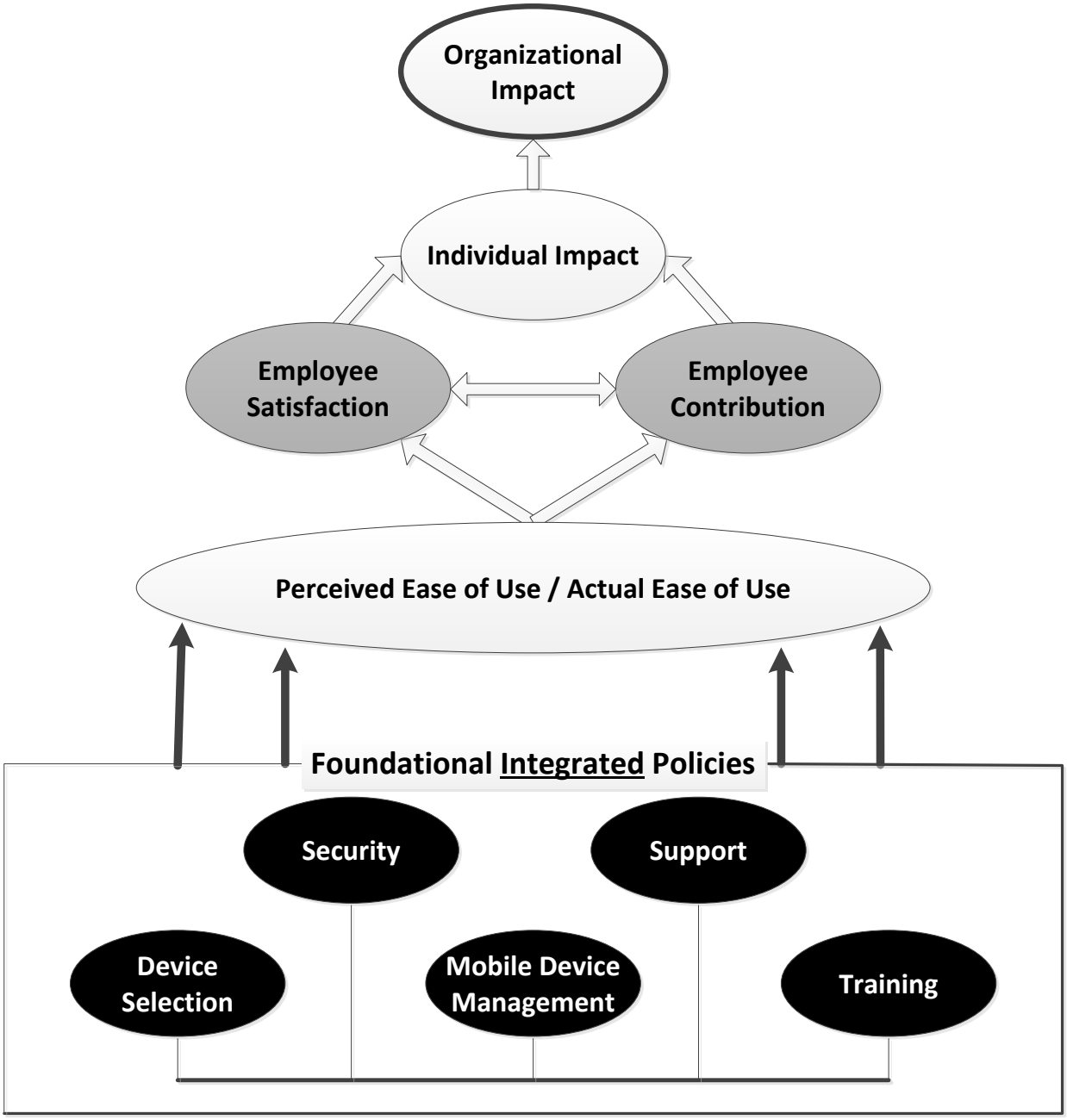

Figure 4: The BYOD Success Model

Increase employees' efficiency, they will usually not take the time to use it. With BYOD, if an organization's policy strongly supports ease of use, employees will use the BYOD program and comply with the program policies. In the case study organizations, employees were even willing to contribute financially to purchase of the devices.

It should be noted of the distinction between "perceived" and "actual" ease of use. Both are important. Similar to the marketing process that promotes a product, raises customer expectations, and then delivers the actual product, perceived ease of use is an absolute must at the beginning of the BYOD program. Over time, of course, perceived ease of use is directly impacted by reality (the actual ease of use being experienced).

With the foundational BYOD architecture in place, the ease of use experience leads directly to employee satisfaction and contribution. Again, both are important. If an employee is very satisfied with the BYOD device, but is not more productive, the organization gains little. On the other hand, if the BYOD device increases the employee's contribution, but does so at the dissatisfaction of the employee, the end result will be muted productivity increases.

The combination of employee satisfaction and contribution is the primary components of the "individual impact" shown in the BYOD Success Model. The positive individual impacts of BYOD then syndicate to give the organization a positive impact. This is the ultimate goal of an organization adopting a BYOD policy.

Finally, if the model's emphasis on individual impact, as opposed to direct impact on teams, departments, divisions, seems over-emphasized, one must go back to the roots of BYOD. The "YO" in BYOD stands for "your own" which clearly targets personal productivity. Most organizations claim that their individual employees are their most valuable assets. If they truly believe this, then a BYOD program is one way to show it while also likely increasing organizational ROI and profitability.

Conclusion

A BYOD program can most simply be defined as a policy that enables and supports employees using their own personal mobile devices for work. Unfortunately, BYOD has largely remained an informal practice for many organizations and is not being used to its' full potential. By adding mobile devices into an organization without a BYOD plan, an organization's IT infrastructure can become over complicated causing strain on both network resources and support staff. Creation of a formal BYOD program then becomes critical for any organization looking to reap the benefits of IT convergence, explosion of mobile computing, and the integration of office and home activities.

References

Alleau, B., Desemery. J., (2013) Bring Your Own Device It's all about Employee Satisfaction and Productivity, not costs! Retrieved from http://www.capgemini-consulting.com/resource-file-access/resource/pdf/bringyourowndevice_29_1.pdf

Aruba Networks, Inc.; A Definitive Guide of BYOD Retrieved from http://resources.idgenterprise.com/original/AST-0088062_BYOD_Brochure.pdf

Bradley, T., (2011, December 11th) Pros and Cons of BYOD (Bring your Own Device). Retrieved from

http://www.cio.com/article/696971/Pros_and_Cons_of_BYOD_Bring_Your_Own_Device_

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., Buckalew, L., (2012) BYOD: A Global Perspective, Harnessing Employee-Led Innovation. Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf

Buchholz, D., Dunlop, J., Ross, A., (2012) Improving Security and Mobility for Personally Owned Devices. Retrieved from http://software.intel.com/sites/billboard/sites/default/files/downloads/Improving_Security_and_Mobility_for_Personally_Owned_Devices.pdf

Byrne, D., Evered, R., (2012, February) Pre-Evaluating Small Devices for Use in the Enterprise. Retrieved from http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/pre-evaluating-small-devices-for-use-in-the-enterprise-paper.pdf

Caldwell, T., (2012, September) Training-the weakest link. *Computer Fraud & Security* 09/2012; 2012(9):8-14. DOI:10.1016/S1361-3723(12)70091-X

Cisco (2012, April 6th) Schools Plug into BYOD: Mobile Devices Transform Learning at Katy ISD. Retrieved from http://www.slideshare.net/CiscoPublicSector/ciscoedukaty-sd-cs

Cisco Public, (2013) Cisco BYOD Smart Solution: Take a Comprehensive Approach to Secure Mobility. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution_overview_c22-702775.pdf

Cheston, R, W., (2012, August) BYOD & Consumerization: Why The Cloud Is Key To A Viable Implementation. Retrieved from http://www.partnerinfo.lenovo.com/partners/us/resources/downloads/toolkit/BYOD-White-Paper-Cheston.pdf

Chin, D., (2013) Best Practices for Enabling BYOD in Education. Retrieved from http://www.netgear.com/images/Netgear-whitepaper-BYOD_070113_tcm18-77080.pdf

Citrix Systems, (2011) IT Organizations Embrace Bring-Your-Own Devices. Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/it-organizations-embrace-bring-your-own-devices.pdf

Citrix Systems, (2013) Best Practices to make your BYOD simple and secure. Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf

Evered, R., Rub, J., (2010, November) Maintaining Information Security while Allowing Personal Hand-Held Devices in the Enterprise. Retrieved from http://www.intel.com/content/dam/doc/white-paper/intel-it-enterprise-security-maintaining-information-security-while-allowing-personal-handheld-devices-paper.pdf

Fiberlink; The Ten Commandments of BYOD. Retrieved from http://trials.maas360.com/forms/register_service_m.php?id=320

Ho, B., (2013, January) Mobile's Impact on Hosipital IT Security in 2013: how your institution can adapt to BYOD. *Journal of healthcare protection management: publication of the International Associate for Hospital Security* 01/2013; 29(2):120-4

Horwath, J., (2013, April 29th) Managing the Implementation of a BYOD Policy. Retrieved from https://www.sans.org/reading-room/whitepapers/leadership/managing-implementation-byod-policy-34217

IBM Global Technology Services (2012) Developing more effective mobile enterprise programs. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/enw03011usen/ENW03011USEN.PDF

Medcalf, R., Loucks, J., Buckalew, L., Faria, F., (2013) The Financial Impact of BYOD, A Model of BYOD's Benefits to Global Companies. Retrieved from http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD-Economics_Econ_Analysis.pdf

Miller, R. E., Varga, J., (2011, May) Benefits of Enabling Personal Handheld Devices in the Enterprise Retrieved. from http://www.intel.com/content/dam/doc/best-practices/inte-it-it-leadership-benefits-of-enabling-personal-handheld-devices-in-the-enterprise-practices.pdf

Romer, H,. (2014, January) Best Practices for BYOD Security. *Computer Fraud & Security* 01/2014; 2014(1):13-15.

Sweeney, J., (2012, November) BYOD in Education, A Report for Australia and New Zealand. Retrieved from http://i.dell.com/sites/doccontent/business/solutions/brochures/en/Documents/2012-nine-conversations-byod-education_au.pdf

Stieglitx, S., Brockman, T., (2012) Increasing Organizational Performance by Transforming into a Mobile Enterprise_ *MIS Quarterly Executive* 01/2012; 11(4):189-204.