Spring 1-15-2013

# Consumerization of IT

Thomas Stagliano
*La Salle*, staglianot1@student.lasalle.edu

Anthony DiPoalo
*La Salle University*, DiPoaloa1@student.lasalle.edu

Patricia Coonelly
*La Salle University*, pcoonelly917@yahoo.com

# The Consumerization of Information Technology

INL 880 – Summer 2012

Prepared By: Tom Stagliano

Anthony DiPoalo

Patricia Coonelly

# Table of Contents

I. Introduction .......... 3

A. How is Mobility Changing the Way Organizations Do Business? .......... 4

B. Embracing the Trend .......... 6

II. The Support and Manageability of the Mobile Workforce .......... 10

A. The Key Strategic Areas to Focus on with Mobility Strategies .......... 10

B. The Acquisition, Tracking and Managing of Mobile Devices .......... 13

C. The Service Desk and the expectation to service Employee's Devices .......... 15

D. Mobile Device Support Solutions .......... 16

E. Policies and guidelines to help organizations embrace mobility .......... 17

III. Security and Controls .......... 24

A. Risk Assessment of Consumer Devices .......... 24

B. Regulations .......... 26

IV. Employee Performance .......... 27

A. How Employees can Adopt to New Technology Trends .......... 28

B. Generating Employee Creativity .......... 30

C. Negative Impact on Employee Performance .......... 31

D. Protection of User and Organization .......... 32

V. Conclusion .......... 33

A. Organizational Readiness .......... 33

B. Summary of Proposed Solutions and Best Practices .......... 36

C. Guidelines for Implementing BYOD .......... 37

D. Lessons Learned .......... 41

Bibliography .......... 43

# I. Introduction

The popularity of smart phones and tablets is growing exponentially as the price of the technology is decreasing and more people are realizing the benefits of flexibility and instant access that is provided by mobile devices. With the rapid growth of mobile devices, employees may soon be requesting the option to use privately owned mobile devices in the workplace. At the same time, the proliferation of mobile devices in the work place has presented a huge challenge to management. Due to the impending shift to mobile devices, the consumerization of IT has become the subject of considerable interest in the Information Technology (IT) industry. The consumerization of IT or “Bring Your Own Device” (BYOD), as it is commonly referred to, is a strategy for allowing employees to choose and purchase their own technology to perform daily business tasks. These devices in question are not organization issued or owned but rather personal devices, which the employee uses in their home or on the go, and which connect to the enterprise’s network. Devices in a BYOD environment can range from smart phones and tablets to personal laptops. The anticipated benefits behind a BYOD initiative are increased productivity, lower corporate cost, and less technical training for employees.

The IT industry needs to define a best practices approach to implementing a “Bring Your Own Device” infrastructure and strategies for the business to support the trend and change the way business is conducted. Organizations are faced with questions regarding the exponential growth of smart phones and tablets, and defining the best practices and key considerations for supporting a BYOD initiative for an organization.

Many IT managers and top level executives may already be in the process of determining how to integrate these consumer products into their environments. IT managers need to be aware of protocols that must be followed and the extent and expectations needed to support the devices.

To successfully implement a BYOD strategy, organizations need to develop and enforce policies and guidelines for these mobile devices.  More importantly, the organization needs to determine what type of support will be provided for user owned devices.

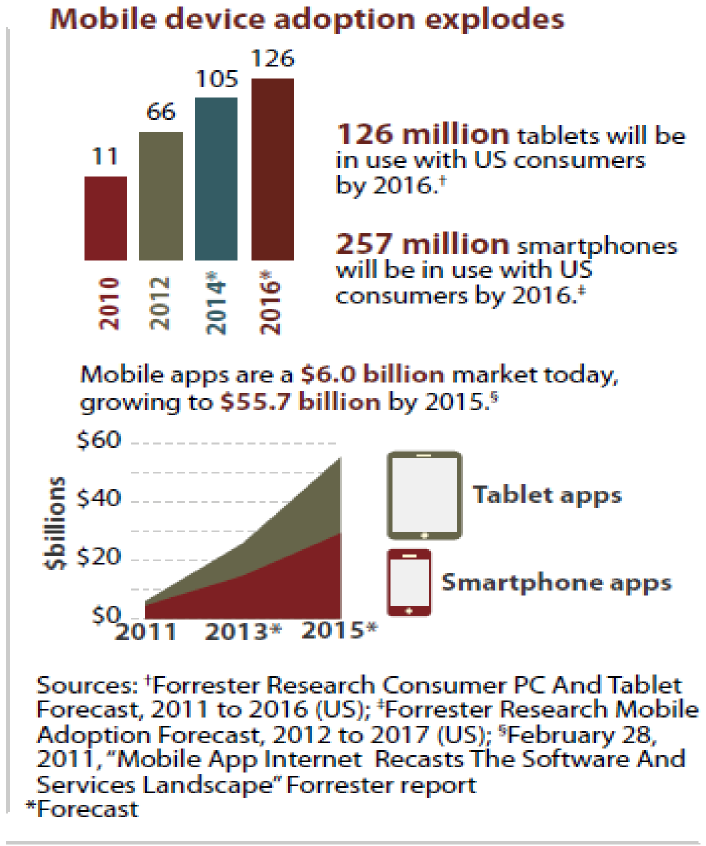
## A. How is Mobility Changing the Way Organizations Do Business?

Employee-owned devices may already be entering the workplace and changing the way business is being conducted.  The possible shift from corporate-owned devices to privately-owned devices could already be underway and the strategy is more complex than just bringing an iPad into the office.  Mobile devices are allowing consumers to interact and become engaged with brands, information and each other all in the palm of their hand.  The applications on mobile phones and tablets are considered systems of engagements.  Systems of engagements differ from traditional business systems; the focus on the systems of engagement moves from processes to customers.  Let's consider a customer wishing to eat at their favorite Mexican Restaurant, El Camino.  The customer can use the GPS context on their mobile phone and can notify anyone of their location via a social media platform; the process is referred to as "checking in".  If the customer checks in to El Camino several times, the app will alert the restaurant.  In turn, El Camino will then reward the frequent customer with a free appetizer of fried pickles.

Let's also consider Quick Response Codes (QR Codes), which are a type of matrix barcodes that have the capability to hold large data.  QR codes are now being used by emergency workers to quickly access health information.  California residents can now put information regarding their medications into a website called Lifesquare then place a QR code sticker where emergency responders will be able scan it with a smart phone or tablet to access their health information. The sticker will provide paramedics with a secure link to the vital information they need during a medical response call (Davis 1). Mobile phones are entering the workforce and the power may be shifting from organizations to consumers since the consumers now have a variety of interesting and useful technologies at their disposal.

Tablets and smart phones are exploding in the market place. In 2010, 11 million tablets were in use and Forrester Research projects the growth of tablets to reach 126 million consumers in 2016 (Shandler and McCarthy, 2). The research provided by Forrester also forecasts that one billion consumers will have a smart phone by 2016 and 200 million employees will bring their own mobile device to work (Shandler and McCarthy, 2). The growth of mobile devices is shaping the mobile market. The driving force behind the growth of the mobile market is the high demand for smart phones and tablets. Figure 1 illustrates the explosion of smart phones and tablets in the marketplace. This chart demonstrates the explosion of new and expanding mobile technologies, which is something that could require businesses to alter the way organizations conduct their daily business activities.

**Figure 1: The Explosion of Smart phones and Tablets in the Market Place (Shandler and McCarthy, 3)**



Mobile device adoption explodes

126 million tablets will be in use with US consumers by 2016.[†]

257 million smartphones will be in use with US consumers by 2016.[‡]

Mobile apps are a $6.0 billion market today, growing to $55.7 billion by 2015.[§]

Sources: [†]Forrester Research Consumer PC And Tablet Forecast, 2011 to 2016 (US); [‡]Forrester Research Mobile Adoption Forecast, 2012 to 2017 (US); [§]February 28, 2011, "Mobile App Internet Recasts The Software And Services Landscape" Forrester report
*Forecast

.

## B. Embracing the Trend

Fueled by the growing popularity of mobile devices, IT managers realize BYOD is not a passing trend and organizations are seeking strategies to engage this trend. Large organizations, such as CARFAX, Kraft Foods, and Proctor and Gamble, offer their staffs enticements to bring their own mobile devices into the office. For example, CARFAX offers their staff an interest-free loan for new computers while Kraft's strategy is to let employees purchase their own PCs. Proctor and Gamble's strategy is to allow its employees to use their own laptops in the office (CDW, 7). Additionally, Citrix Systems realized a BYOD strategy could result in a reduction of capital expenditures and instead of using organization issued laptops, it provides their employees a $2,100 stipend which allows their employees the freedom to buy and use a notebook of their choice (CDW, 7). Non-traditional organizations, like Citrix, are realizing the increased benefits of mobile technology and are introducing strategies to embrace the trend rather than limit it.

Osterman Research believes that employees may be able to use their various mobile devices to do work as BYOD accommodates a flexible work style (Osterman, 6). Employees are no longer constrained as to when and where they can access corporate resources. Employees can better organize their time because mobile devices enable greater flexibility and may increase productivity. Furthermore, mobile devices serve as a great coup to business processes as it can equip the sales force with accurate numbers or provide service workers with the availability and scheduling of parts (Mobile Enterprise, 4 -5). Embracing a BYOD strategy may allow employees greater freedom, real-time data, and could simplify the work life by combining many aspects of work and mobile. Organizations could conceivably see an increase in productivity from employees away from the office as well as on weekends.

Aside from major productivity gains an organization may see through anytime access, research from Apperian concluded a BYOD strategy could keep current employees happy. BYOD may serve as an effective recruiting and retention tool to attract the best and brightest professionals (Apperian, 5). A mobile strategy may invoke a positive morale in employees and could add value to an organization by blending functions together and allowing employees to operate more efficiently. BYOD improves morale by acknowledging the growing trend to use the devices employees want instead of the devices the organization wants them to use in the workplace. It also acknowledges that both business and personal life need constant attention.

In the current economic climate, there is increased pressure to tighten budgets and lower costs. Organizations which adopt a BYOD approach expect to see lower support costs due to the personal responsibility an employee may feel over the device, and in some scenarios, an employee may try to fix the device first before calling the service desk (CDW, 3). Budget limitations are forcing organizations to think more strategically. A BYOD initiative is an alternative to help reduce costs and help the organization cope with the downsizing of IT support staff. The integration of employee's devices in the workplace minimizes the time spent learning and managing new tools used by the organization. Employee-owned devices in the workplace could help reduce IT support costs and may help organizations stay within budget constraints. However, prior to implementing a BYOD program, organizations need to understand the costs involved. While there may be savings long term, there will be initial startup costs, and if organizations are not careful, they may not realize long-term savings but could actually see an increase in their technology costs.

Organizations should see their overall technology costs decrease over time. One factor for a decrease in technology costs is that there should be less of a need for desktop computing devices since employees will be using their own. For example, if employees are utilizing their own mobile devices such as a smart phone or slate/tablet, there should be less of a need for an organization to purchase the employee a laptop; a desktop PC should suffice which is a significantly lower cost than a laptop and typically has a longer lifecycle.

Another factor which could lead to a decrease in technology costs is that organizations should be spending less for cellular phones, since employees will be using their own smart phone devices. It is a practice in many organizations, that if employees purchase the device, then the organization pays for the monthly service plan. This is a good trade-off for an organization, since smart phones typically cost $150-$200.  In order for this to be successful in cutting costs however, organizations need to ensure that the mobile plans are optimized and that unnecessary fees or services are not being charged to the organization or the overall costs increase.  To help to further contain costs, it is a good practice for organizations to re-negotiate their wireless plans often, or at a minimum, annually.

Although there are cost reduction opportunities to a BYOD offering, there are also hidden costs that an organization may incur.  The following are examples of hidden costs that an organization should consider.

**Figure 2: BYOD Hidden Costs**

| Hidden Costs of a BYOD Program |
|---|
| Increased Telecommunications Charges: The additional bandwidth needed to provide connectivity for the devices |
| Cost of additional Wi-Fi access points: Needed for the devices to connect within organizations locations |
| MDM costs: Including license fees as well as the hardware costs to house the MDM solution |
| Security breaches or loss of intellectual property (IP) through theft of loss of a device: Is addressed through an MDM solution |

Aside from the benefits of decreased IT costs, organizations should embrace the BYOD trend because based on the research conducted by Shandler and McCarthy, organizations can expect that systems of engagement could act as a catalyst for the reinvention of IT as business technology much like how the PC necessitated an organizational shift from data processing to IT (Shandler and McCarthy, 13).  Naturally, mobile devices could become a catalyst in the reinvention of IT as a business tool.  The paradigm may conceivably shift in the near future and mobile devices could facilitate a need for top managers to reconsider information technology strategy in their organization.  Mobile devices are possibly a stepping stone for a much broader portfolio of new systems of engagements.

## II. The Support and Manageability of the Mobile Workforce

### A. The Key Strategic Areas to Focus on with Mobility Strategies

Plenty of opportunity could exist for a mobile workforce, but what are the key strategic areas to develop a mobility strategy?  Foremost, do not approach BYOD from an ad-hoc basis; organizations may need to adopt a formal strategy to control the influx of personal devices.  To fully reap the benefits of a BYOD environment, such as flexibility, productivity, and cost reduction, a comprehensive mobile strategy is essential for a successful implementation.  A mobility strategy with proper governance reduces perceived threats and risks associated with employees using their own devices.

Ultimately, mobility is part of a broader end-user productivity strategy.  Lauren Jones, a senior principal analyst for Deltek's Federal Market program, says organizations should identify the conditions under which it makes sense for workers to have laptops, versus desktops or tablets or smart phones (ProofPoint, 4).  Through careful analysis of business processes, an organization can figure out where mobile computing makes the most sense and more importantly, provide a competitive edge to the organization.  The first step in this process is to build a task map.  A task map helps IT managers become familiar with the tasks and the workflows that will be processed on the employee's mobile device so that the device can deliver the functionality needed to get their duties done.

Another key strategic area to focus on is the role of the CIO. The CIO plays a critical role in spearheading the consumerization of IT strategy. He/she leads the organization through the experimental phase and proceeds into a structured progression toward systems of engagements. The switch to BYOD often comes from other stakeholders, specifically the Chief Financial Officer. The shift in technology could also change the nature of the CIO's relationship with the CFO. The CIO, with the support of the CFO, may approach the other senior level executives as partners in business-investment decisions because provisioning new technologies is a strategic initiative based on business and financial goals.

The CIO is accountable for the integration of mobile products and services into the business environment along with limiting mobile services which introduce risk to the organization. Realizing mobile technology is transforming business, SAP CIO, Oliver Bussmann, established a device-agnostic strategy for his organization (SAP, 5). Under Bussmann's leadership, SAP successfully implemented a BYOD initiative and today it supports the four major platforms of iOS, BlackBerry, Android, and Windows Mobile. The consumerization of IT is currently being deployed at SAP as the organization is allowing employees to bring their own device to connect to their corporate networks. Currently, SAP has 22,000 BlackBerry smart phones in use and more than 8,500 iPhones. Upon the release of the iPad, the organization immediately rolled out 1,000 iPads and now has 18,000 iPads in use today (SAP 5). Top level leadership teams could look to SAP, CARFAX, and Kraft Foods to see how they embrace BYOD. To remain vital in the reformation of IT, CIO's may need to help develop mobile architectures and manage mobile technology investments.

From research conducted by Shandler and McCarthy, it is not wise to approach mobility from a project standpoint as a project approach to mobility will result in escalating costs, slower growth of their mobile engagement IQ, and damage to the organization’s brand if the app suffers due to systems failure; a dedicated mobile technology group will mitigate these problems (Shandler and McCarthy, 15). To coordinate business and technology, organizations should consider establishing the office of the Chief Mobility Officer (CMO) and a supporting mobile team.

Based on organizational size, the office of the CMO may be comprised of 10 to 30 person group that has a diverse range of skills in both business and technology, including financial planning, user-experience design, program management, and process analytics. This special team is responsible for coordinating all the mobile business projects and establishing the mobility culture throughout the organization. Team members do not need to be permanently assigned to the group; some group members may be on a six month or twelve month rotation. The mission of this group is to focus on the language of business especially when the BYOD initiative is just beginning or when the project is critical to the business.

In the initial phase of the mobility strategy, the office of the CMO should conduct an assessment to identify all the mobile technologies and projects currently in the organization. Shandler and McCarthy indicated the importance of a mobile assessment citing, one organization found that it had more than 100 mobile projects under way while another organization discovered that it was supporting 114 different versions of the BlackBerry operating system (Shandler and McCarthy, 16). In their assessment of the projects already in process, the team should make a record of the stakeholders, the systems the project impacts, and how it is funded. The primary responsibly of the team is to share information regarding application design, development and system integration. The primary objective of the Office of the CMO is to bridge business and technology together.  It is their duty to establish the engagement culture in the organization.

## B. The Acquisition, Tracking and Managing of Mobile Devices

To procure mobile solutions, organizations should employ a strategic sourcing method. Shandler and McCarthy recognized that employees pay for more than half of the devices and data plans used for work across every region (Shandler and McCarthy, 3).  Their research also indicates the same holds true for tablets: Employees pay for 70% of the tablets used for work (Shandler and McCarthy, 3).  The research conducted has shown smart phones and tablets are valuable enough on the job that employees will buy their own devices to use at work.  For many organizations, a mobility strategy strives to reduce the number of devices issued to employees. By shifting device ownership to employees, it decreases the need to procure organization issued desktops, laptops, and mobile phones.

Organizations must agree on the types of devices they are willing to let into their corporate environment.  A self-service portal would provide employees with procurement information.  This approach was recommended by Sam Gross, VP of Global IT Outsourcing Solutions at Unisys.  He justifies his approach by explaining that a portal may not only put a corral around the “Wild West” of technologies, but could also make the employees feel empowered that they have choice, which in turn may increase productivity and lower costs at the same time (All, 8).  Organizations should poll their employees on preferences of mobile devices and then present them with a predetermined list of permitted devices and applications along with providing the employee with required equipment standards.

Organizations allowing employees to procure their own devices should take into consideration the lifecycle of mobile devices. Specifically, the lifecycle management of mobile devices is part of a much broader Mobile Device Management policy, which will be discussed in the policies and guidelines available to organizations to help them embrace mobility. However it is important to note there is no clear model for the useful life of a mobile device but the length of time is rapidly falling due to advances in new mobile technology.

To track the cost of mobile devices, organizations need to implement a mobile expense management strategy. In SAP's adoption of a BYOD environment, the organization implemented mobile expense policies that regulated the direct costs associated with business mobility. The policies SAP implemented defined allowances and expense reimbursements for employees, established an approved list of carriers and permitted rate plans that were appropriate for specific job functions, and stated usage when travelling internationally (SAP, 10). Through a mobile expense management process, organizations may be able to manage and control the costs of the organization's mobile communications network as well as avoiding employee misuse of the organization's mobile systems. The strategy should maintain the organization's use policy regarding employee's mobile devices. Mobile expense management can be assisted through software or it can be a part of a larger system such as a Mobile Device Management System. Organizations may also approach mobile expense management by implementing a digital allowance. Under this strategy, organizations will share the cost of the device and reimburse up to a certain amount for employees to buy their own technology for work.

Aside from tracking costs, organizations also need to track the usage on the network bandwidth. Usage policies should be implemented at the WLAN access point or wired point. By adopting the usage policies at network edge, organizations may be able to effectively direct traffic to the correct destination, limit bandwidth, handle specific network protocols different ways and deliver application services without requiring traffic to be sent back to a centralized controller for policy enforcement (Enterasys, 6).

Mobile devices may increase the usage and activity on the network and organizations should plan accordingly. For successful management of mobile devices, organizations should institute a usage and compliance policy. A usage policy is a crucial factor in the BYOD deployment because end-user's activities on their devices may affect the overall performance of the network. Under the policy, organizations would be able to control what resources are available to end-users and prioritize delivery of the information based on the users' need. Organizations should define usage policies based on factors such as device, location, and time of day.

## C. The Service Desk and the expectation to service Employee's Devices

A well-equipped service desk is one of the primary components for a successful rollout of a mobility strategy. The BYOD environment is constantly changing. The service desk should plan for various versions of mobile devices to support. The changing nature of mobile devices has necessitated a need for organizations to plan for the future. To help with the influx of new devices and also prepare themselves for an influx of new applications and new clients, organizations should consider implementing a centralized management platform like OneFabric Control Center. OneFabric Control Center provides the service desk with deep visibility and instant access to troubleshoot on the organization network by providing a user profile with information such as user name, device, location, and IP address and also a drill down feature once the problem has been identified to help discover and fix the problem.

The researchers at Mobile Enterprise concluded that device configuration and remote control capabilities may enable support personnel to resolve support requests with very little time or effort on the part of employees (Mobile Enterprise, 3). Organizations should consider applying a remote support strategy that provides instant communication with support personnel via a web or application based chat. A centralized helpdesk for all mobile devices and a shared point of contact for both application and device support will increase end-user productivity and streamline routine tasks for technicians. The technicians have a centralized view of an employee's device, which will make it easier to trouble shoot the source of the problem.

## D. Mobile Device Support Solutions

Additionally, restricting the use of additional applications on the device via organizational policies is not a practical solution. One approach to resolve this issue is to automate policy management through a Mobile Device Management system (MDM). An MDM system provides controls that managers need to enforce policies and manage network access based on several factors including but not limited to user, device, and location, time of day, port, and authentication type.

The deployment of an e-rich support solution is recommended for a broader platform of support. This will equip the support technicians with the tools to simulate and see exactly what the end-user sees as opposed to relying on their description of the problem. A one to one remote interaction between a technician and an end-user is the best method for resolving unpredictable problems, such as removing a virus, because it will allow the technician to interact with the device. It is also suggested that organizations simulate various platforms as new mobile applications are being made and it will also be helpful when those rogue devices happen to crop up in the organization. Furthermore, it is important that an organization implements a strong support system for the reason that it will help safeguard the advantages in the BYOD initiative.

## E. Policies and guidelines to help organizations embrace mobility

Organizations do not have to look far to find good mobile policy management. Enterasys has highlighted an example of a good mobility policy and governance in an enterprise setting. They recommend redirecting the clients to the guest portal to register their devices. The organization is essentially capturing all of the mobile devices being used by the employee on the organization's network. The employee has access to the corporate e-mail servers, intranet, internet, but is restricted to secure resources such as the corporate database. To limit traffic from external sources Enterasys recommends limiting the download rate to any mobile device during normal business hours except perhaps in the conference rooms.

Mobile technology is moving very quick and organizations need to prepare for a new era of mobile device management. Preparation includes developing a mobile device management policy for employee owned devices. Lax governance rules regarding mobility will lead to non-compliance issues and data breaches. Mobility policies should include a baseline on the hardware that the organization is willing to support and restrictions on devices such as blacklisted applications or jail broken phones, which are smart phones that have been tampered with to allow users to gain root access to the operating system to customize the device. Device policies should be based on grouping already in the organization such as departments. The guidelines should be documented in organizational policies and communicated to the employees who wish to participate in the BYOD program. In turn, the employees should be required to acknowledge that they understand the policies and the guidelines. The contract between the employee and the organization should feature specific requirements directed by the internal stakeholders of the organization.

The costs of the MDM tool will vary, based on the need as well as the number of devices to support.  Since the mobile computing market is constantly evolving, the costs for MDM solutions are also quickly changing based on needs.  The costs will be not only for the MDM software itself, but also for the hardware to house and run the software and for IT administrative staff to manage the platform.

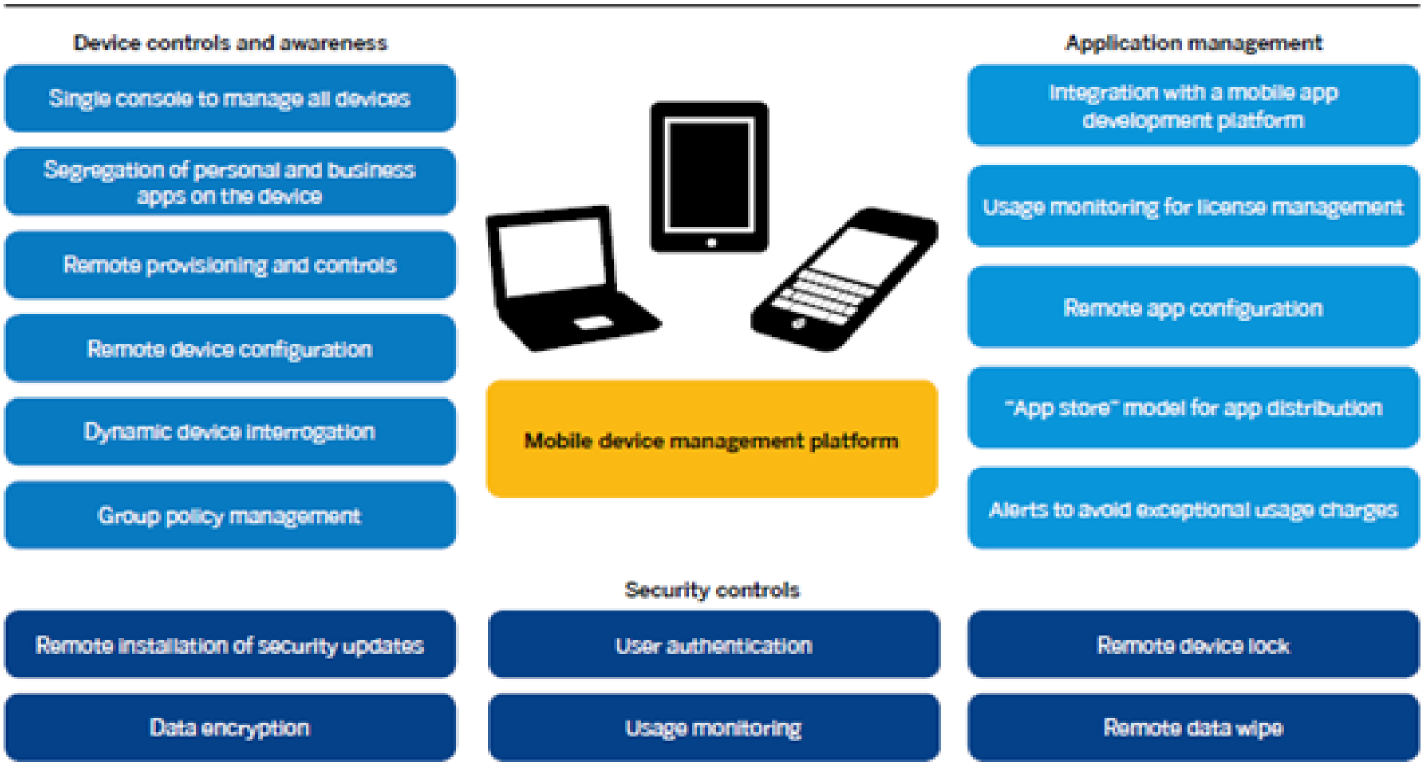
Although organizations might initially see an increase to their overall costs in the short run due to their investment in an MDM solution, organizations can greatly benefit from the tool as the system will manage and control user-owned devices at the client level.

An MDM platform can also enforce policies concerning the lifecycle management of mobile devices.  Based on the research from The Enterprise Mobility Foundation, mobile device management should be considered the operations component of the mobile hardware lifecycle. (The Enterprise Mobility Foundation, 3).  The lifecycle management will be a key component in the protection of corporate assets and the proper MDM platform will ensure hardware is performing in line with specific lifecycle policies and specifications. MDM can support lifecycle management of the mobile devices throughout the organization.  It will enable the automation of device enrollment, monitoring and de-enrollment of the employees' devices. An effective policy includes the on-boarding, retiring, and replacing of mobile devices.

Figure 2 further demonstrates the additional capabilities of an enterprise grade mobile device management platform (SAP, 11). As the chart suggests, the functionalities of the MDM system can be broken down into three categories consisting of device controls and awareness, security controls and application management. Under the device controls and awareness, there will be a single console to manage all mobile devices. This functionality will allow organizations to support the latest and greatest mobile devices as the MDM platform will be compatible with a variety of mobile operating systems (SAP, 11). As part of device controls and awareness, an MDM platform should enable an automatic enrollment process of mobile devices. During the automatic enrollment process, the MDM system may display an acceptable use policy and issue a device certificate before continuing on to provisioning the device over the air in addition to applying device settings, security policies, and applications (Phifer, 20). The automatic enrollment process begins with the on-boarding of the employee's device. For initial access to the corporate networks, employees can follow a link to a self-help enrollment portal where the employee will be required to enter the device specifications. The MDM system then authenticates the user and compares the user and device to predefined IT policies for the organization. If the user is allowed to register the device based on the credentials of device, such as make/model, ownership and group membership, access to the corporate network will be granted. The automatic enrollment feature allows for scalable support and clear boundaries on acceptable use of mobile devices. Group policy management or group membership, is also a key functionality of an MDM platform as it will support remote device control based on group policies.

For security controls, the functionality of an MDM platform will allow management to continually monitor activity and enforce policy compliance. To mitigate the risks associated with mobility, the MDM solution can also temporarily remove settings that allow a device to access corporate e-mail, VPN or application access. An MDM can also be used to remotely configure device settings to reflect the organization's security policies, including requiring a PIN or password, enable automatic lock or wipe features, and encrypt data on the device (Phifer, 20). The automatic wipe feature of MDMs can also distinguish between a full device-wipe and enterprise wipe. The enterprise wipe would allow the organization to discharge an employee's mobile device without sacrificing any personal data. The two different wipe capabilities are a critical functionality of an MDM platform because a major concern for management is the integration of private data with sensitive corporate data on an employee-owned device. In the area of application management, organizations must manage the applications on the employee-owned devices. The MDM platform will allow the IT department to have the ability to manage and support applications through deploying, installing, updating and deleting, and blocking of applications on the end-user's device. The MDM platform will also be able to segregate business apps from personal apps. The remote provisioning and control capabilities will enable IT managers to remotely configure devices in addition to providing automated security controls. An effective MDM platform will allow employees to leave personal applications, pictures, and data intact while also controlling corporate data and business applications in the event that the employee leaves the organization or loses their device. Many MDM platforms permit administrators to selectively wipe the contents on the device and allow the administrator to distinguish between corporate data and personal data. The application management capabilities of the MDM platform will also allow organizations to push applications to remote devices over the wireless network and alert employees of data usage that exceeds the data plan for their device (SAP, 11). The usage monitoring feature provides information regarding device type, versions of the mobile operating system, software licenses in use, and other critical information. Using the broad functionalities of an MDM platform will enable organizations to manage their mobile devices in a strategic way (SAP, 11).

**Figure : Mobile Device Management Capabilities (SAP, 11)**


Device controls and awareness
Single console to manage all devices
Segregation of personal and business apps on the device
Remote provisioning and controls
Remote device configuration
Dynamic device interrogation
Group policy management
Mobile device management platform
Application management
Integration with a mobile app development platform
Usage monitoring for license management
Remote app configuration
"App store" model for app distribution
Alerts to avoid exceptional usage charges
Security controls
Remote installation of security updates
Data encryption
User authentication
Usage monitoring
Remote device lock
Remote data wipe

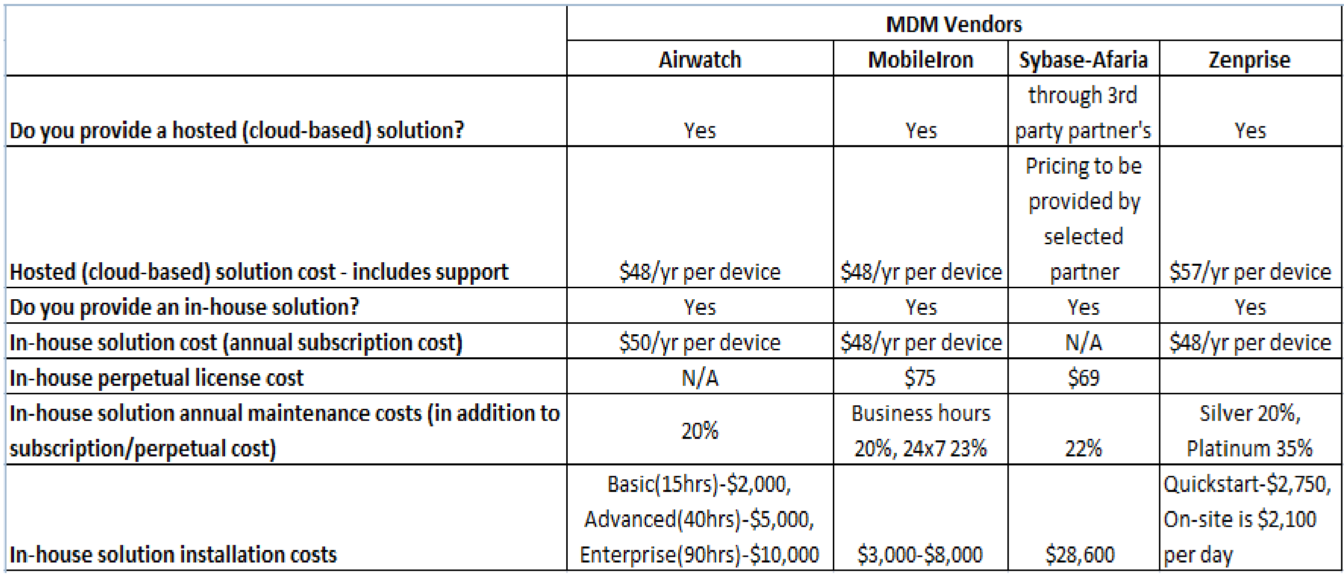
Initially organizations will more than likely need to make an investment in an MDM solution to help them support BYOD types of devices. The costs of the tool will vary, based on the need as well as the number of devices to support. Enterasys explains that MDM can greatly reduce business risks for applications and corporate data resident on the consumer device by controlling and protecting the data and configuration settings on the mobile devices in the network (Enterasys, 7). MDM will secure sensitive corporate data, while at the same time, it will monitor, manage and support mobile devices throughout the organization. At the present time, organizations can use a MDM solution to manage devices running on Apple's iOS 4+, Android 2.2+, and a variety of devices running on WinCE and Windows Mobile.

Since the mobile computing market is constantly evolving, the costs for MDM solutions are also quickly changing based on needs. Some MDM vendors offer cloud and even hosted solutions that could prove to be a lower cost than if an organization directly administers the tool themselves. Four major MDM vendors were selected to contrast features and costs: Airwatch, MobileIron, Sybase (Afaria), and Zenripise.

Based on our research these 4 vendors have very similar capabilities. In the area of device control awareness, all 4 vendors offer centralized management and offer an automatic enrollment process which can display an acceptable use policy. During the enrollment policies, all 4 of the MDM solutions push a certificate to the device. The certificate is used by the MDM console to communicate to the device. Sybase is the one vendor of the 4 whose enrollment policy includes mandatory acceptance of an acceptable use policy; the other vendors donot make the acceptance mandatory. In the area of application management, all 4 vendors offer automated installation of applications, and all offer white listing and black listing of applications. In the area of security controls, all 4 vendors all offer very similar security policies. All offer remote wipe capabilities, including locating and wiping lost or stolen devices, and each offers a level of isolating corporate data including the ability to wipe corporate data only. Zenprise appears to offer a better job than the other 3 vendors at a selective wipe. iOS device wipes consist of wiping anything that was pushed by Zenprise to the devices and Android device wipes remove anything that was pushed to the device from Zenprise within a container that is created by Zenprise on Android devices.

Regarding costs, all 4 vendors have a similar pricing structure. The following table shows a comparison of costs for the selected MDM vendors

**Figure 4: MDM Vendor Cost Comparison (B. Ziegler, personal communication, April 12, 2012)**



| | MDM Vendors | | | |
|---|---|---|---|---|
| | Airwatch | MobileIron | Sybase-Afaria | Zenprise |
| Do you provide a hosted (cloud-based) solution? | Yes | Yes | through 3rd party partner's | Yes |
| Hosted (cloud-based) solution cost - includes support | $48/yr per device | $48/yr per device | Pricing to be provided by selected partner | $57/yr per device |
| Do you provide an in-house solution? | Yes | Yes | Yes | Yes |
| In-house solution cost (annual subscription cost) | $50/yr per device | $48/yr per device | N/A | $48/yr per device |
| In-house perpetual license cost | N/A | $75 | $69 | |
| In-house solution annual maintenance costs (in addition to subscription/perpetual cost) | 20% | Business hours 20%, 24x7 23% | 22% | Silver 20%, Platinum 35% |
| In-house solution installation costs | Basic(15hrs)-$2,000,<br>Advanced(40hrs)-$5,000,<br>Enterprise(90hrs)-$10,000 | $3,000-$8,000 | $28,600 | Quickstart-$2,750, On-site is $2,100 per day |

Lastly to help organizations embrace mobility, The National Institute of Standards and Technology (NIST) is establishing guidelines on the mobile device security. The guidelines for Managing and Securing Mobile Devices in the Enterprise were released in July 2012 and open for public comment until August 17, 2012. The standard will be designed to explain threats and countermeasures available to organizations. The standard uses a multilayer approach to protect against data breaches and data loss. Identity management control is used to properly authorize access to the enterprise's resources. This includes passwords and other authentication measures, device account lock out, automatic lock after a period of idleness, and remote lock if the device has been unlocked in an unsecure location. For organizations to allow employees to bring their own technology to work, top managers must make policy decisions and mitigate the threats from mobile device access.

# III. Security and Controls

BYOD offerings have thus far been a "quandary" for IT departments to support, with the quandary being that IT will not be able to treat these devices like the organization now "owns them" and secure them in the same way they do with organization purchased equipment; they will need to treat BYOD devices differently (Ginovsky, 24). IT must continue to protect and secure an organization's information, and enable functionality for clients to meet business objectives. These two goals are not always in sync. From a support standpoint, security has been among the greatest concerns for IT departments in that area of BYOD. A recent study by CompTIA showed that security concerns are the greatest risk that IT has in support for mobile devices (Ginovsky, pg. 25).

## A. Risk Assessment of Consumer Devices

One of the risks associated with employee owned devices is that applications which are downloaded to these personal devices could introduce vulnerabilities including viruses and malware to the device and extend it to the enterprise. Additionally, employees can transfer corporate data to their personal device, which could lead to stealing of corporate data when the employee leaves the organization, or data loss, should the device be lost or stolen. Furthermore, these devices are typically used over wireless networks, which are inherently less secure than a corporate network. Wireless networks are less secure because anyone who is in range of the signal of the wireless network can try to access it, whereas you would need physical access to a wired network to access it. To secure a wireless network, strong encryption should be implemented. All of these risks will need to be assessed when IT organizations decide on a strategy to support personal devices. The following table shows a listing of other possible risks associated with mobile devices and means to mitigate these risks.

**Figure 5: Mobile Device Risks**

| Risk or Threat | Mitigation Strategy |
|---|---|
| Use of Untrusted Devices | Secure the device via MDM solution |
| Use of Applications Created by Unknown Parties | Restrict which applications can be installed via an MDM solution |
| Interaction with Other Systems | Restrict which devices or systems the mobile device can sync to via MDM policy |
| Use of Untrusted Content | Implement a security awareness training program |
| Use of Location Services | Turn off GPS services via MDM policy |

The shifting paradigm of utilizing personal devices in the workplace requires IT departments address the reality that personal data such as family photos and music that have been purchased will reside on these devices, and that implementing a policy such as auto-wipe a device after a password has been incorrectly entered “X” number of times will not be practical. There need to be procedures to deal with these types of scenarios. There is a way to “lock down” a device via an approach known as “containerization” where the organizational data resides within that a container or partition of the device and cannot interact with personal data. The most common containerization MDM offering is from Good Technology. This approach however changes the client experience significantly, possibly to the point where the user may lose interest in utilizing the device. There are less intrusive MDM solutions for IT to consider such as the offerings by Air Watch or Zenprise. While these solutions retain the same user experience as a non MDM managed device, they only take the policies offered by iOS, Android, and any other platforms that may be in use and roll them up into one console for IT administrators to manage the devices, rather than having a separate management console for each device vendor. These solutions do not offer their own policies or security options, nor do they provide IT with the level of control that it has been used to with devices that an organization directly owns. IT and the users both share in the responsibility of securing the devices. Offering an effective security awareness program to the users within an organization will provide a better security mechanism than trying to lock the devices down to the point where they are no longer useful. Examples of simple and effective tips include the following:

- Reminding users to physically secure their device as much as possible when traveling,
- Utilizing a password on a device which would lock the screen due to inactivity,
- Using encryption on the devices if at all possible.

Organizations do not wish to be highlighted on the front page of the Wall Street Journal due to a data security breach caused by a BYOD enabled smartphone or tablet, therefore there must be a balance between security practices and user productivity on these types of devices.

## B. Regulations

As an IT organization develops a strategy to support mobile devices, the organization needs to be adhere to the framework and controls of regulatory acts such as Sarbanes Oxley (SOX) for publically traded organizations, Payment Card Industry (PCI) for organizations who accept payment transactions via credit card, and the Health Insurance and Portability and Accountability Act (HIPAA) for with the healthcare industry. The Payment Card Industry Data Security Standards Council has a set of guidelines to deal specifically with mobile technology. The guidance is designed to help merchants and acquiring banks to understand their responsibilities under PCI and how these responsibilities translate to mobile payment acceptance.

While it is true that BYOD devices will need to comply with the appropriate regulations and standards in the area of information security, the actual level of security will differ depending on the industry.  For example, a device used by a government worker or worker in the financial services industry will need to be secured to a greater level than a device for someone in a manufacturing organization or marketing firm.  If an organization is a multi-national organization, then there will be additional concerns to consider, such as that it is illegal for an organization to format or wipe a personally owned device.  While there is no such litigation in the U.S. that prohibits the wiping of a personal device by an organization, many U.S. based organizations are now global and the differing country regulations about employee owned devices will need to be investigated and implemented.

## IV. Employee Performance

With a combination of the mobility move, the newer generation of employees and the BYOD trend, the IT world is changing drastically from just a few years ago.  New technologies are appearing in users' everyday lives both at home and at work, which are causing IT professionals to re-think how they support these technologies.  According to Ted Shandler and John McCarthy, "By 2016, smartphones and tablets will put power in the pockets of a billion global consumers." (Shandler and McCarthy, 2)  More and more employees have a stronger desire to utilize their own personal devices for work, thus businesses should consider taking advantage of this opportunity and embrace this trend as it is becoming increasingly popular very quickly.  According to IDC, "employee-owned smartphones will represent more than half (56%) of the business smartphones shipped in 2013, for a total of 56.7 million devices going into the hands of individual workers in the next three years." (Employee-Owned Smartphones, 1)  As with any new initiative, an organization needs to weigh both the pros and cons of implementation not just from the technology side, but also from the employee performance perspective.

## A. How Employees can Adopt to New Technology Trends

Assisting with leading this new trend of BYOD is what is being called "Millennial Generation" or "Generation Y". Ryan Faas describes this group as "the first generation that grew up with broadband internet access, mobile phones, and social networks and it shaped their lives and expectations in important ways." (Faas, 1) This group is the future of the current workforce, and the BYOD trend is attracting interest from organizations eager to provide the necessary tools and policies to allow the workers to use these devices and technologies. This allows organizations to eliminate the amount of training on the new mobile devices because they are very knowledgeable about these technologies already. Once these younger workers are comfortable with the devices in the workplace, they can take a mentor approach to train their coworkers on the usage of these devices. They become advisors to the organization rather than the IT department. Since IT departments will not be needed to develop training programs for the organization at a mass level, this will in turn reduce the training cost needed for such programs.

Since the newer mobile devices are targeting the consumers rather than business staffs, users tend to become comfortable with their own devices which they have had for several months and are sometimes unwilling to either carry around multiple devices or reluctant to learn a different business targeted device. In the end, BYOD allows the users to be comfortable with a device they already know how to navigate and are very knowledgeable on how to utilize the business applications that are presented to them. They will be more eager to adopt and utilize those applications, instead of learning the mobile devices first and then the applications.

Organizations will save money on hardware costs for additional devices to be purchased due to these employees purchasing their own devices.

With the ever changing enhancement in the mobile devices technologies, the Generation Y group has become very enthused in adopting new technologies when they become available in the market which in turn will translate into a deeper commitment to the mobile strategy that organizations are trying to deploy. If there is no user acceptance in such a strategy, then organizations are wasting valuable time, money and resources to develop these strategies. According to a study conducted by Ann Bednarz on organizations who allow personal mobile devices to access the corporate networks, "46.2% said the policy has increased productivity among end-users. A nearly similar number (47.2%) said it has increased end-users ability to work from home." (Bednarz, 2) When employees become productive the organization usually gains from that productivity and they also gain a sense of accomplishment because the policies created relevant to the new mobility trend are successful. Similar policies can also be seen with a dollar figure being placed on the BYOD trend. Matt Hamblen noted a Cisco study that, "estimating productivity gains with workplace use of consumer devices of between $300 and $1,300 annually depending on the worker." (Hamblen, 1) Even though such productivity gains are appreciated by the organization, when employees see their hard work being rewarded, they strive to be more creative, efficient and even more productive.

Having a very interactive and collaborative workforce makes for an enjoyable workplace for everyone as there is less hostility, anger or stress among colleagues. With the Millennial Generation assisting with training, they also strive to research problems on their own rather than always bothering the already overworked and busy IT department that it makes them a valuable asset to any organization. When new projects arise and a team is formed which consists of a few members of the Millennial Generation, they are very eager to collaboratively work with other colleagues while utilizing their mobile devices to the best of their ability to assist the team with being successful.  When they do encounter issues with their mobile devices and they spend the time to research the problem and define a possible solution, with the accessibility of wiki and social networking sites like Facebook and Twitter, they become a library of solutions that are being shared amongst not only their team, but the global workplace.

## B.  Generating Employee Creativity

With increased productivity comes increased morale and a sense of pride in the workforce that all the work employees are performing and the tools they are using are allowing them to perform their job at the highest level with the greatest amount of success.  With this sense of pride, employees are more eager to take ownership of any new processes and technologies they are using to perform their job.  They may become more satisfied in their current role and strive to continue to perform well and improve their position in their organization.  Morale building is a key component in keeping a good workforce intact for many years as they strive to work well to be successful.  What the BYOD trend allows these employees to do is utilize their similar devices as others to find the best approach to resolve a problem which in turn makes the organization look good.

As noted earlier in this research, the mobile technologies are changing rapidly with newer versions of smartphones with enhanced features and functions that are geared toward those who utilize their smartphone to perform business tasks.  Since organizations usually have to supply these smartphone devices to a very large number of users, these same organizations tend to drag their feet in implementing the newer devices thus making the workforce behind in the newest trends. Consumers themselves tend to adopt newer devices much quicker than an organization thus allowing them to stay ahead in these trends and be in line with the rest of the global consumer workforce. These newer devices allow the business tools already deployed in the organization to be more accessible in multiple ways and on multiple devices.

## C. Negative Impact on Employee Performance

Today's devices are programmed to allow the end-user to multi task between a variety of functions such as e-mail, social networking, and playing games, and organizations need to control the amount of time their employees spend on their own devices playing games during the work day instead of doing actual work. There are times throughout the day where it will be warranted to have a little downtime to check personal e-mails or even play a game like Angry birds or Words with Friends, but the employee needs to respect the organization's time vs. personal time. Too much time may also be wasted on streaming live videos and music during the work hours. There are more risks associated to this then just wasting time throughout the day which include the viewing of inappropriate videos that could be classified as not safe for work or listening to music that contains violent or offensive language which could offend other colleagues around the office resulting in disciplinary action.

With employees utilizing their own devices, they do not make their personal cellular phone number available to other coworkers, but all personal contacts of these employees still have the opportunity to call that employee during the day. Again there are times when this is warranted when there is a family emergency or a situation at the employee's home that needs to be discussed right away which is understandable to the organization, but there is a risk of an excessive amount of incoming and outgoing calls that can be distracting from the daily job. This is also true of sending and receiving text messages as well as checking updates made to their Facebook or Twitter accounts.  Since these devices provide full access to these applications at any time of day, the temptation is to continually check their message board so they feel as nothing is being missed in their social lives while they are at work.

## D. Protection of User and Organization

Although the trend for organizations to allow their employees to bring their own devices into the workplace sounds like a good idea, there are a number of risks that need to be considered before fully implementing this initiative.  Organizations need to consider the risks "stemming from the loss, unauthorized use, and/or viral infection of such devices; comprise of confidential information; litigation; damaged reputation; findings of noncompliance by examiners; and more." (Ginovsky, 24)  Security is one of the biggest challenges organizations need to be concerned with due to the ever growing BYOD trend.  Security involves the biggest risk for not only the individual to get into trouble, but also the organization.  According to John Ginovsky, "Organizations will have to strike a balance between business objectives and security objectives, which may not always be in sync." (Ginovsky, 26)  They do not want to completely block all functionality on these devices for their users as this will cause frustration on the user's part thus forcing them to ignore the usage of such devices and finding other means to accomplish their job.  When employees are restricted to perform certain tasks, those that are technically proficient will leverage any other technological device at their disposal to get their job finished which could bypass all policies and procedures the organization already has put into place to safe guard the employee and the data of the organization.

Organizations today have a very large amount of information that is very confidential to their business and is what makes them competitive in their market place. They develop very complex security procedures to protect this data. The sensitivity of this data is very important and when organizations introduce initiatives that allow their workers the ability to access this confidential information at any time from any location in the world, they become very strict on who can access this information, in what manner and from what means. The employees need to understand how sensitive this information is so they can access it properly outside of the office and continue to perform their job. Not only do these employees have to be educated on the security of data, but also how to properly secure their devices and what best practices the organization developed to assist. If these best practices are not followed, the organization could be in grave danger of their data being available to the public eye and their competitors. Organizations need to develop policies and guidelines to adopt mobility, but at the same time these same guidelines must protect the organization when an employee is terminated and all organizational data and applications need to be cleared from the personal device to assure the employee has no connection to the organization once they are terminated. There are many instances where a disgruntled employee who still has access to organizational data, either deletes very important data or corrupts a certain data set which causes widespread harm to the organization’s systems.

# V. Conclusion

## A. Organizational Readiness

The consumerization of IT in the workplace has created a tremendous opportunity for organizations to allow their employees to work in newer, more productive ways than ever before.

Before organizations can adopt such trends, their IT departments will need to revamp their model for support from an application support help desk to a more device centric service desk.  Before officially adopting any new policies and procedures, an in-depth piloting program should be developed to allow the organization to prove the value and viability of the new BYOD model. According to Good Technology, creating such a pilot program will allow organizations to "study the implications of the policy in action, alter it, and expand when appropriate." (Good Technology, 11)  Such a program will allow the IT Departments to obtain real and concrete data to show upper management that this trend is a reality and their attention is needed.

With the BYOD trend, the service desk will become more knowledgeable on the hardware side of these new devices, but that will not be their main purpose for support to their end-users.  Since these are the user's personal devices, when they have an issue with their device or its OS or experience poor network coverage, the employee must go to their vendor directly to resolve it.  (Good Technology, 13)  This will keep the organization's IT department more focused on enforcing and maintaining the BYOD policies.  These departments have very limited ability to resolve device, OS or carrier issues, but if the IT department detects a trend on certain issues or errors being reported from their end-users, they will be able to direct those employees to a more reliable carrier that supports the similar devices the users are currently using in the workplace.

The BYOD trend is approaching quickly on organizations and they should adhere to these changes instead of neglecting them.  As noted by Good Technology in their Practical Guide for Implementing BYOD programs in an organization, they mentioned that one approach to assist with adhering to the changes brought upon by the BYOD trend is by developing a logical workflow which will document and communicate any BYOD approvals for the users.  Such a workflow will deliver one result to the users: “a more efficient, more secure, and less costly mobile communications environment.” (Good Technology, 12) This workflow will clearly identify who in the organization is responsible for approvals related to BYOD. Automating such a process can also have its benefits in that IT Departments can “keep support time and costs to a minimum, allowing them to focus on more strategic programs and projects.” (Good Technology, 12) Once a logical workflow is developed and deployed, communication becomes a critical success factor for organizations to adhere to the changes in the BYOD trend. Plan changes, device changes, expirations of plans, early termination fees and policy changes must all be communicated in a clear, standardized fashion. (Good Technology, 14) There are a number of communication channels available which organizations can use to broadcast such messages like e-mail, newsletters, blogs, corporate websites, and organizational intranets that will allow all users utilizing the BYOD trend to stay informed and receive the same message as to eliminate confusion.

IT Departments should strive to accommodate and support the fact that employees are buying new devices and want to use them at work. (Good Technology, 15) Since the technology on these devices is changing very rapidly and the end-users are becoming smarter in using them, organizations must protect the corporate data without interfering with the personal use of these devices for the end-users. There are more implications to consider other than technical, such as legal, financial, business process and human nature when developing BYOD policies and procedures. The old mindset for IT departments to say “no” to every employee who asked to access corporate data on their personal device is being dissolved as these same employees will find workarounds to the policies set in place because they are smart people with smart devices. For the BYOD initiative to be truly successful, organizations need to incorporate a robust technology solution with effective policies, processes and communication methods to ensure the safety of the organization and those  employees who work there.

## B. Summary of Proposed Solutions and Best Practices

For a best practices approach to implementing a BYOD initiative, organizations can look to SAP's Global IT team.  SAP decided to implement a BYOD strategy to address the consumerization of IT trend of allowing employees to use their personal devices to connect to corporate resources.  The Global IT team at SAP can be credited for the development of a rock-solid mobile deployment and security strategy (Bussman, 9).  First, SAP offered their employees the option to use either a corporate owned or personally owned device for work.  SAP offered their employees the option to purchase their mobile device through a corporate catalog or buy their own devices from an approved list.  Employees then accessed a self-service enrollment page to connect their devices to SAP's MDM system, which automatically installed e-mail and the VPN configuration and applied security policies (Bussman, 9).  SAP has chosen to support their devices through a mobile wiki, where employees can modify the content through the browser.  Information regarding the support for the device is constantly being updated and improved as SAP employees make their contributions to the wiki community.  Support for mobile devices can also be achieved through a centralized and well-equipped service desk.

It is important to note that SAP required all data that is stored on all devices to be always encrypted.  The IT department can stay constantly aware of all types of threats to employee's mobile devices through an MDM system.  SAP uses Afaria's MDM system, which allows their IT department visibility into the device.  Those devices which are compromised are denied access to their corporate network.  Afaria allows SAP to centrally deploy, configure, and manage their multiplatform mobile devices whether the devices are personally owned or organization purchased (Bussman, 9).

SAP had a successful rollout of a BYOD initiative because they had a sound mobile strategy. As SAP CIO, Oliver Bussman, noted the key considerations for a successful implementation for organizations considering mobile technology, are security and management (Bussman, 9). The security and management of the technology must be incorporated in the initial mobility strategy as well as in each stage of the mobile lifecycle. Organizations should approach a BYOD strategy with strong corporate governance policies that emphasize security and should frequently educate their employees on how to adhere to the policies and procedures the organization executed regarding the use of their personal devices in the workplace.

## C. Guidelines for Implementing BYOD

This research has explored the best practices approach to implementing a “Bring Your Own Device” infrastructure as well as the strategies for business to support the trend and possibly change the way business is conducted. The rapid growth of smart phones and tablets has allowed employees and organization to realize the benefits of flexibility and instant access that is provided by mobile devices. The research conducted showed explosion of new and expanding mobile technologies and how it could possibly alter the way organizations could conduct their daily business activities. Mobile devices are allowing employees to interact and become engaged with brands, information and each other through a variety of interesting tools such as QR Readers and the GPS context on their mobile device.

With the possible shift to user-owned devices, organizations need to determine what type of support will be provided for employees' devices. The research conducted stressed the need for organizations to agree on the types of devices they are willing to support and more importantly, let into their corporate environment. Through careful analysis of business processes, an organization can figure out where mobile computing makes the most sense and more importantly, provide a competitive edge to the organization. Research showed that a mobility strategy with proper governance will reduce perceived threats and risks associated with employees using their own devices. Through a self-service portal, an organization will be able to provide employees with procurement and support information. For a successful roll out of a BYOD environment, organizations should have a well-equipped service desk. The service desk will be able to help with the influx of new devices and should plan for various versions of mobile devices to support.

Furthermore, an organization must invest in an MDM system to help manage BYOD. A MDM solution will provide controls that managers need to enforce policies and manage network access. The MDM solution will enforce policies and guidelines that will help organizations embrace the BYOD trend. An MDM will also help mitigate the security risks involved with utilizing BYOD, but IT and the users both share in the responsibility of securing the devices.

There are many security risks involved with utilizing BYOD such as introducing vulnerabilities like viruses and malware into organization. Additionally, employees can transfer corporate data to their personal device, which could lead to stealing of corporate data when the employee leaves the organization. Organization should also keep in mind that data loss is extremely high should the device be lost or stolen. Furthermore, these devices are typically used over wireless networks, which are inherently less secure than a corporate wired network.

When it comes to cost and expenditures of implementing a BYOD initiative, corporations should not expect an immediate reduction in IT costs. While there may be savings long term, organizations will be faced with initial startup cost. The danger in the startup cost is if organizations are not careful, they could actually see an increase in their technology costs. Most likely, an organization will need to invest in an MDM tool. The costs of the tool will vary, based on the need as well as the number of devices to support. The costs for the hardware to house and run the software should also be factored into the budget as well as an IT administrative staff to manage the platform. Through a mobile expense management process, organizations may be able to manage and control the costs of the organization's mobile communications network as well as avoiding employee misuse of the organization's mobile systems.

BYOD is worth the investment as it will improve employee's performance. The trend allows organizations to eliminate the amount of training on the new mobile devices because employees are very knowledgeable about these technologies already. BYOD allows employees to be comfortable with a device they already know how to navigate and are already very knowledgeable on how to utilize the business applications that are presented to them. Employees may show more eagerness to adopt and utilize those applications, instead of learning the mobile devices first and then the applications. A BYOD environment could conceivably foster a very interactive and collaborative workforce, which makes for an enjoyable workplace for everyone as there is less hostility, anger or stress among colleagues. And as previously stated BYOD will also generate more employee creativity and increased productivity.

The challenge in a BYOD initiative is the organization needs to determine what type of support and security will be provided for user owned devices since the organization does not technically own these devices. As stated previously, from a support standpoint, security has been among the greatest concerns for IT departments in that area of BYOD. The IT department cannot treat these user-owned devices like the organization's regularly purchased equipment. The issue is that IT departments must continue to protect and secure an organization's information while also at the same time enable functionality for clients to meet business objectives. Security is a major hurdle to overcome in a BYOD initiative.

Another issue IT managers face is the negative impact on employee performance. Today's devices are programmed to allow the end-user to multi task between a variety of functions such as e-mail, social networking, and playing games. Organizations need to control and regulate the amount of time their employees spend on their own devices playing games during the work day instead of doing actual work. It is possible that employees may waste too much time on streaming live videos and music during the work hours.

For organizations to allow employees to bring their own technology to work, top managers must make policy decisions and mitigate the threats from mobile device access. Below are guidelines that an organization should consider in moving towards a BYOD plan:

- Do not approach BYOD from an ad-hoc basis. Adopt a formal strategy to control the entry of personal devices.
- Give employees the option to use either a corporate owned or personally owned device for work and provide employees with the option of either purchasing a mobile device through a corporate catalog or buy their own devices from an approved list.

- Create a self-service portal or enrollment page that will register employee's devices and capture all of the mobile devices being used by the employee on the organization's network
- Implement an MDM system to enforce policy and protect against perceived threats.
- Employ a well-equipped service desktop to provide support for the device
- Establish the office of the Chief Mobility Officer (CMO) and a supporting mobile team to coordinate all the mobile business projects and to create the mobility culture throughout the organization.

## D. Lessons Learned

The main lesson learned from researching the BYOD trend is to embrace the consumerization of IT and use an effective strategy with strict policies to control the influx of personal mobile devices in the workplace. The research has concluded that mobile devices can allow employees to interact and become engaged with brands, vital information and each other all in the palm of their hand. BYOD may change the way business is conducted by providing employees with greater freedom, real-time data and simplifying work-life balance. Nontraditional organizations who embrace BYOD can conceivably see greater productivity and increased morale in employees.

For a successful BYOD implementation organizations need to corral "the Wild West" and determine what type of support will be provided for user owned devices. An important lesson taken from this research is that security will be a big challenge to organizations wishing to implement a BYOD environment. To help mitigate the risks organizations can offer an effective security awareness program to the users within an organization that will provide a better security mechanism than trying to lock the devices down.

Since BYOD is still in its infant stage and rather new to most organizations, the next piece of research to consider is measuring the success of corporations who have implemented a BYOD initiative like SAP or Kraft Foods.  Research conducted could include measuring the value of increased employee productivity throughout the organization.  Such an experiment would allow the IT managers to obtain real and concrete data to show upper management that this trend is a reality and their attention is needed.

## Bibliography

“*Best Practices for Mobile Device Support*” http://www.itwhitepapers.com/index.php?option=com_categoryreport&task=thankyou&title=17968&pathway=no&gen=0&pi=1668444&cfmurl=http%3a%2f%2fforms.madisonlogic.com%2fFormConfirmation.aspx%3fpub%3d88%26pgr%3d75%26src%3d6851%26cmp%3d4854%26ast%3d17968%26frm%3d300%26embed%3d1%26up%3d2-1668444-33-5-57-321-0. [Last Accessed June 1, 2012].

“*Bring your own device. Individual Liable User Policy Considerations*”, Good Technology, 2012 VISTO Organization and Good Technology

“BYOD: Cost Saver Not Curse”, CDW Editorial, July 19, 2012

*“Proof Points”*.http://www.i360gov.com/whitepapers/tracking-the-use-of-mobile-technologies-in-government/ [Last Accessed June 1, 2012].

“Securing Mobile Devices. August 2010. An ISACA Emerging Technology White Paper 2011. Retrieved 6/2012

All, Ann (2010).*How to Handle Support for Employee-Owned Technology*. [ONLINE] Available at: http://www.itbusinessedge.com/cm/blogs/all/how-to-handle-support-for-employee-owned-technology/?cs=44043. [Last Accessed June 1, 2012].

Bednarz, Ann, “*BYOD: The Inmates of the asylum have control*”, Network World, April 19, 2012

Bradley, Tony, “Pros and Cons of Bringing Your Own Device to Work”, Dec 20, 2011

Bulkeley, Bill, (2011). The New Budget Conversation: Cloud computing and Consumerization of IT change how you buy and budget for technology. Here's how to talk about it with the CFO. *CIO*. 24 (14), pp.N/A

Bussman, Oliver (February 2012). “*Going Mobile at SAP*”, Available at:
Crosman, Penny, “*Banks and Bring Your Own Computer Might Work*”, Bank Systems & Technology, May 10, 2010, http://www.banktech.com/blog/archives/2010/05/banks_and_bring.html

Davis, Kerry, “*Emergency Workers Scan QR Codes to Quickly Access Health Information*”, CIO, May 30, 2012, pg.1, Available at: http://www.cio.com/article/707327/Emergency_Workers_Scan_QR_Codes_to_Quickly_Access_Health_Information

Delaney, Darragh, "*Implementing a BYOD policy on your network*", ComputerWorld, May 30, 2012

Duffy, Jim, "*Cisco helps users welcome BYOD*", Network World, Mar 26, 2012, 14

Enterasys (2012).*Bringing Order to the Chaos of "Bring Your Own Device"*. [ONLINE] Available at: http://searchconsumerization.bitpipe.com/detail/RES/1338399983_87.html. [Last Accessed June 1, 2012].

Fogarty, Kevin, "5 Things You Need to Know about BYO Tech", *CIO Magazine,* December 16, 2010

Gibilisco, S. (2011).*Mobile Expense Management*. [ONLINE] Available at: http://searchfinancialapplications.techtarget.com/definition/mobile-expense-management. [Last Accessed June 1, 2012].

Ginovsky, John, "*BYOD quandary*", American Bankers Association. Aba Banking Journal, April 2012, 24

Gittlen, Sandra, "*A sampling of BYOD user policies*", Network World, April 2, 2012

"*Bring Your Own Devices Best Practices Guide: A Practical guide for Implementing BYOD Programs at Your Organization"*. Good Technology. 2011

Hamblen, Matt, "*Consumerization trend creates IT worries, worker benefits*", ComputerWorld, May 18, 2012 http://fm.sap.com/mobilesense/. [Last Accessed July 1, 2012].

Information Week.p. 45.Retrieved 6/2012

Kanaracus, Chris, "*IBM CIO embraces BYOD Movement*", Computerworld, April 9, 2012

Kenyon Paul. "Four IT Security Trends to Master". May 2012. The Risk Management Society.Retrieved 7/2012

Kovacs, Gary, "*Bring your own device to work is finally here*", CNN Money, September 1, 2012, http://tech.fortune.cnn.com/2010/09/01/bring-your-own-device-to-work-is-finally-here.html

Messmer Ellen. "*Federal IT Pros Look at BYOD Security, Management Concerns*". April 5, 2012 http://www.networkworld.com/news/2012/040512-BYOD-feds-258024.html Retrieved 6/2012

Nash, Kim S, (2011). The BYOD Buzz: Kraft, Whirlpool, Motorola Solutions and other employers are pioneering BYOD policies to drive productivity and reduce costs. Here's why your employees want this and what you need to do to make it happen.*CIO*. 25 (1), pp.N/A

Osterman Research, "*Embracing and Empowering the Consumerization of IT*." August 2011, http://www.itwhitepapers.com/index.php?option=com_categoryreport&task=thankyou&title=18906&pathway=no&gen=0&pi=2417739&cfmurl=http%3a%2f%2fforms.madisonlogic.com%2fFormConfirmation.aspx%3fpub%3d88%26pgr%3d75%26src%3d2449%26cmp%3d3549%26ast%3d18906%26frm%3d300%26embed%3d1%26up%3d2-2417739-27-6-70-321-0. [Last Accessed June 1, 2012].

Phifer, L., (2012). BYOD: Taming the Tide. *Information Security*. 14 (4), pp.16-22

PR Newswire, (2011). Absolute Launches the World's First Document Control App for iOS to Allow Organizations to Manage the Security Risks of the Consumerization of IT. *PR Newswire*. (), pp. Retrieved 5/2012

SAP Whitepaper (March 2012). "*Managing Mobile Devices in a Device-Agnostic World Finding and Enforcing a Policy That Makes Business Sense*", Available at: http://research.pcworld.com. [Last Accessed July 1, 2012].

Shandler, Ted; McCarthy, John (February 13, 2012). "*Mobile Is The New Face Of Engagement*." Available at: http://www.itbusinessedge.com/offer.aspx?o=03430192search. [Last Accessed June 1, 2012].

The Enterprise Mobility Foundation (2011).*Looking Beyond Mobile Device Management*. [ONLINE] Available at: http://docs.media.bitpipe.com/io_10x/io_103696/item_506440/Looking_Beyond_Mobile_Device_Management.pdf. [Last Accessed June 1, 2012].

Wallin Leif-Olan. "Gartner's View on Bring Your Own in Client Computing". Oct 20, Week.p. 12.Retrieved 6/2012

Westervelt, R., (2012). Solving the BYOD Problem. *Information Security*. 14 (4), pp.9-10

Wittmann Art. "BYOD? First Get Serious About Data Security". Nov 14, 2011.

Wittmann Art. "Can IT Be Trusted With Personal Devices?" May 28 2012. Information

Zielinski, Dave, "*Bring Your Own Device: More Employers are Allowing Employees to Use Their Own Technology in the Workplace* ", HR Magazine, February, 2012