Fall 1-15-2014

# Strategically Addressing the Latest Challenges of Workplace Mobility to Meet the Increasing Mobile Usage Demands

Shweta Somalwar
*La Salle University*, somalwars1@student.lasalle.edu

Loc Nguyen
*La Salle University*, nguyenl14@student.lasalle.edu

# Capstone Project:

# Strategically Addressing the Latest Challenges of Workplace Mobility to Meet the Increasing Mobile Usage Demands

INL 880 – Fall 2013

La Salle University

Prepared by: Shweta Somalwar and Loc Nguyen

January 3, 2014

# Table of Contents

# 1 Executive Summary

During this post-PC era, many organizations are embracing the concept of IT consumerization/ Bring-Your-Own Device (BYOD) in their workplace. BYOD is a strategy that enables employees to utilize their personally-owned mobile devices, such as smart phones, tablets, laptops, and netbooks, to connect to the corporate network and access enterprise data. It is estimated that employees will bring two to four Internet-capable devices to work for personal and professional activities. From increased employee satisfaction and productivity to lower IT equipment and operational expenditures, companies have recognized that mobile devices are reasonably essential to their own success.

However, many organizations are facing significant challenges with the explosion of mobile devices being used today along with provisioning the appropriate supporting infrastructure due to the unprecedented demands on the wireless and network infrastructures. For example, there is not only a growth in the number of wirelessly connected devices but the amount of bandwidth being consumed on the enterprise networks as well which is furthermore driven by increased usage of video and enterprise applications.

Managing mobility and storage along with securing corporate assets have become difficult tasks for IT professionals as many organizations underestimate the potential security and privacy risks of using wireless devices to access organizational resources and data. Therefore, to address the needs and requirements of a new mobile workforce, organizations must involve key members from the Information Technology (IT), Human Resources (HR) and various business units to evaluate the existing and emerging issues and risks posed by BYOD. Then a mobile strategy should be developed by taking into consideration the enterprise objectives to ensure it aligns with the overall organizational strategy.

There are various solutions available to address the needs and demands of an organization, such as Distributed Intelligence Architecture, network optimization, monitoring tools, unified management and security platforms, and other security measures. By implementing a suitable mobile strategy, organizations can ensure their particular enterprise network and wireless architecture is designed for highly scalability, performance and reliability.

They must also evaluate their existing policies and procedures to ensure appropriate security and privacy measures are in place to address the increasing mobile usage demands and potential liability risks.

By taking these factors into consideration, our team has analyzed the current BYOD issues for Educational Testing Service (ETS), which is a non-profit organization based in Princeton, New Jersey. Our findings have revealed a few major technical concerns relating to inadequate network and wireless infrastructure and the lack of a unified management and security platform. Thus, the team has recommended for ETS to implement Distributed Intelligence Architecture, network optimization and Enterprise Mobility Management (EMM) to address and resolve their current issues and risks.

In conclusion, companies are beginning to seize this transition in order to become competitive and productive in the workplace; however the unprecedented demands on the corporate network and risk to data security are critical aspects that need to be evaluated on an on-going basis. With this analysis, organizations can review, evaluate and implement the proposed solutions and best practices to address the most common BYOD-related issues that companies are facing these days. However, organizations should continually research the latest technologies that may be available and implement solutions that specifically meet their issues.

# 2 Introduction

## 2.1 Paying Attention to the Mobile Explosion and the Usage Demands

Mobile devices have become more persistent in businesses today than in previous generations of computing (desktops and laptops). Mobile applications are used for both personal and business purposes and thus are driving the likeliness of a single device being used for different types of communications. According to the research group, Forrester Research, Inc., it is estimated that by 2016, 350 million workers will use smartphones — 200 million of whom will take their own devices to the workplace (Yahoo, 2013). These devices and their applications have become common tools for today's workforce, and are being integrated into the daily business processes and operations of organizations, improving productivity and becoming a critical, yet complex, component of the computing environment. At the same time, mobile devices have become more and more powerful, often exceeding PC performance, application diversity and capabilities found in organizations today (Johnson, 2012). Due to this, users are increasingly purchasing a variety of mobile devices to meet their everyday needs, and thus the total number of mobile devices around the world will continue to increase.

> *According to recent statistics gathered by Forrester indicate that there will be **1 billion** smartphone customers by 2016 (Panzarino, 2012).*

A few years ago, the ratio of network-enabled devices per user was about 1:1(Kerravala, 2012). Now, it's more common today for a single user to have multiple devices such as smartphones, tablets, and other mobile devices in the workplace, pushing the ratio to 3:1, and it's predicted to grow to a ratio of 7:1 by 2016 (Kerravala, 2012). Even with no employee growth, IT

can expect to deal with 300 percent more devices now and plan for 700 percent growth over the next three years (Kerravala, 2012). Many more devices will be connected to the network by the same employee or person, often simultaneously, and lead to a large increase in overall connected devices. Consequently, while mobile devices are not new to the enterprise, simply the volume of devices connecting to the enterprise is overwhelming. The devices are only a fraction of the challenge as the mobile usage demands are requiring many organizations to become prepared for the mobile demands. This is especially true for a non-profit organization called Educational Testing Service (ETS) that is based in Princeton, New Jersey. ETS is a company that is in the early stages of BYOD adoption, and due to the high interest and demands of the employees, it has decided to expand the program's availability within its workforce. ETS understands that BYOD has the potential to increase worker productivity, create a more flexible working environment, and even reduce IT costs, however ETS also realizes that BYOD can raise critical network, data security and privacy concerns. Thus, it will require an evaluation of its current infrastructure to determine the security holes and areas for improvement. This is a critical step in the process because the BYOD phenomenon has begun reshaping the way IT is purchased, managed, delivered, and secured. And because it is part of the growing IT consumerization trend, IT leaders cannot ignore it (Detwiler, 2013). According to Cisco, it is estimated that mobile devices and the traffic they create on enterprise networks will increase by 26X between 2010 and 2015, driven by more powerful smartphones and tablets, with users demanding Internet access and access to applications wherever and whenever they want (Cisco, 2013).

These issues combined with the explosion of mobile devices being used today can lead to potential legal and liability risks as well. Many companies are playing catch-up to control these risks. It is also the variety and volume of devices being used today that will making the IT

departments struggle. The thought of hundreds of thousands of devices accessing the enterprise network can be enough to keep IT managers and CEOs up at night—and with good reason. Between faulty hardware, hackers, and common human error (lost phones, for example), enterprise mobility can expose an organization to network, security and compliance risks. Organizations, like ETS, must evaluate their existing policies and procedures for device procurement and management, application deployment, and data ownership. In addition, the next generation Internet faces issues handling not just the proliferation of these devices but how they are going to grow and be intelligent enough to continue providing ubiquitous connectivity. As the mobile explosion leads us further into the mobile computing era, it's imperative for organizations to take a step back and take a hard look at this transformation and assess how it is impacting their overall business and the infrastructure. In addition, organizations should proactively prepare for the increasing demands of workplace mobility by developing and implementing an enterprise mobility strategy.

## 2.2 Background on the Consumerization of IT and BYOD Trend

Mobility is one of the key drivers of technology today, and as a result, within organizations, users are not only connecting corporate-issued laptops, but also a multitude of other mobile devices including tablets and smart phones. In fact, according to a survey conducted by Network World, over 80% of workers surveyed bring personal devices to work, and out of those users, 80% have reported connecting their devices to the corporate network for work-related activities (Strong, 2012). This transformation is known as the consumerization of IT and it has gained tremendous traction with the expectations and abilities of the users, and empowers

them to act on their own. The technology has become so personal and so easy to personalize that it encourages employees' desire to have "their" very own technology. Technology developments haven't caused the consumerization of IT. Consumerization of IT is an expression that explains a deeper shift in workplace expectations, especially among employees (PWC, 2011). It refers to the rising influence that consumer-focused technology experiences have on technology expectations at work (Foley, 2010). Thus, if employees at an organization already have smartphones, use email or own laptops (personal or company-provided), then the consumerization of IT is already present in that organization. The number of workers requesting access to corporate data and applications from their own tablets and smartphones instead of from corporate issued equipment is rapidly increasing. Employees, by using their personal mobile devices at work, are forcing IT to integrate and manage employee-owned and corporate-provided smartphones, tablets, and laptops. This has been leading organizations to embrace the wave of bring-your-own devices (BYOD). This is a strategy which allows employees to utilize their personally-owned devices to connect to the corporate network and access enterprise data.

In the past, businesses drove the pace of technology adoption, but times have clearly changed. By the end of 2012, smartphones had represented over 59 percent of the "smart connected devices" sold worldwide, as reported by International Data Corporation (IDC), a global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets (Bort, 2012). IDC defines the "smart connected device" as laptops, smartphones and tablets. Consequently, it is apparent that the BYOD trend has been growing strongly with no signs of slowing down as employees are becoming more accustomed to using their own mobile devices for both personal and professional activities. The reasons for this include the desire to avoid carrying and managing multiple

devices, to using the most up-to-date devices that exist, and to increasing efficiency (infolawgroup.com.). The swift adoption of high end smart phones and tablets that are continually advancing these days along with the endless count of easily accessible applications is largely driving this concept forward. Mobile devices have changed the way people perform their everyday tasks, and therefore users around the world are eagerly waiting to be the first to purchase the newest innovative technologies. In fact, millions of employees around the world own smart phones and tablets, and due to the functionalities available, they have come to expect anytime, anywhere access on their devices, which is blurring the line between personal and professional activities. BYOD isn't just about giving employees what they want. It's also about the army of devices that have entered the enterprise and how those devices have changed the way employees work.

At the same time, organizations have recognized that mobile devices are essential to their own success because they believe that BYOD will allow them to take advantage of the latest technology features and capabilities, without the pain and expense of a large-scale hardware refresh or software upgrade. When employees choose their own devices, IT spends less time (and money) specifying and purchasing equipment. According to VMware, routine support and help desk overhead that come with device ownership are directed at the retailer, manufacturer or service provider—not corporate IT—and that can lower operational costs and free up resources (VMware, 2013). In addition, a mobile workforce can be an advantage for employers in many ways. Organizations that embrace this concept can realize dramatic increases in employee satisfaction and productivity. Allowing users to choose their own mobile technology will generate considerably more streams of information, which is ultimately beneficial for the organizations. If employees can access the network anywhere, anytime, on the device of their

choosing, limitations of the traditional nine-to-five workday will no longer exist. Therefore, additional benefits to the organizations include the potential for employees to work more efficiently, while also cutting down on monetary and environmental costs.

# 3 Concerns Related to Mobile Usage Demands

## 3.1 Network Impact

### *3.1.1 Growth in Data Usage and Traffic*

Some of the prevalent devices that will challenge an organization's network are smartphones, tablets, and laptops. In 2012, smartphones averaged about 1,600 megabytes of usage per device a month, tablets averaged about 800 megabytes of usage per device a month, and laptops averaged about 2,500 megabytes of usage per device a month, however recently there has been growth in mobile data usage (Cisco, 2013). The first trend is growth in average traffic per device type. Cisco states that the average traffic per device is expected to increase rapidly in 2017 for the devices as indicated in the table below:

**Table 1 - Summary of Expected Growth per Device Type, MB per Month**

| Device Type | 2012 - MB usage per Month | 2017 - MB usage per Month |
|---|---|---|
| Nonsmartphone | 6.8 | 31 |
| M2M module | 64 | 330 |
| Smartphone | 342 | 2,660 |
| 4G smartphone | 1,302 | 5,114 |
| Tablet | 820 | 5,387 |
| Laptop | 2,503 | 5,731 |

*Source: Cisco VNI Mobile Forecast, 2013*

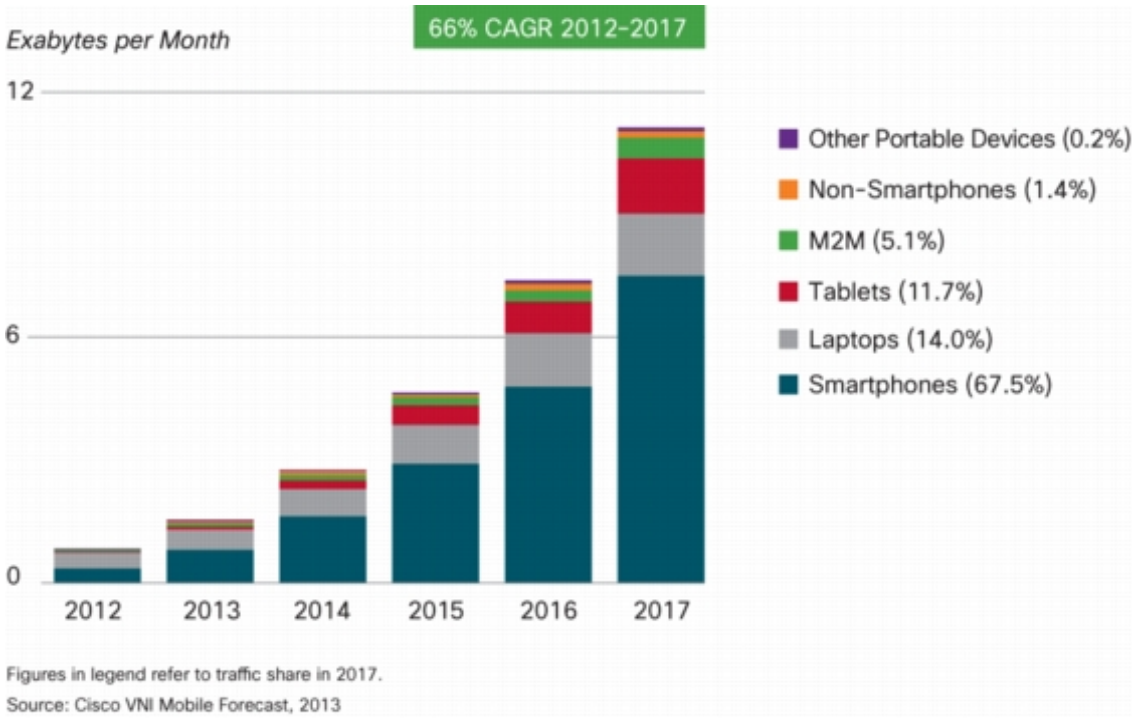
Based on the Cisco forecast, the combination of smartphones and 4G smartphones are expected to grow approximately six to seven times; that amounts to about 7,700 Megabytes (7.7 Gigabytes) by 2017; tablets are expected to grow seven times; that amounts to 5,300 Megabytes (5.3 Gigabytes) by 2017; while laptops are expected to only double averaging to 5,700 Megabytes (5.7 Gigabytes) by 2017. Usage from mobile devices, especially from smartphones and tablets, will impact a network traffic load. In addition, Cisco states the growth in usage per device outpaces the growth in the number of devices. The growth rate of new-device mobile data traffic is two to five times greater than the growth rate of users (Cisco Bring Your Own Device, 2013). The amount of data usage per device will put a strain on an organization's network, potentially causing an impact on business-critical applications.

The second trend is device diversification. A recent study conducted by IDC found that 68% of employee-owned devices in 2012 were being used to access business applications; which is up from 45% in 2010 (Mehra, 2013). The newer mobile devices come in many forms and have the latest technology integrated for wireless capabilities. As these wireless devices are added to the mobile landscape, they are causing an increase in traffic growth. This trend will present

network challenges to an organization that allows employees to use their mobile devices for work-related functions.

Figure 1 below shows the use of laptops was higher for data usage in 2012. However in 2013 smartphone data usage is higher. Smartphones and tablets will account for a significant amount of traffic by 2017. In 2012, these devices along with laptops are accounted for about half an Exabyte per month of traffic. This year, smartphones and other devices account for about 1 Exabyte, which equals to 1,073,741,824 Gigabytes, per month; while laptop traffic only increased slightly by over half an Exabyte. The traffic data growth of smart devices is projected to double to two Exabytes per month by 2014, three Exabytes per month in 2015, six Exabytes per month by 2016 and finally increasing to about eight Exabytes per month by 2017.

**Figure 1 – Mobile Traffic Share from 2012-2017**



During this span, laptops and non-smartphone growth is expected to become gradual as the years go by. Therefore, as projected, smartphone devices will be responsible for more data traffic growth starting now and rapidly increasing every year to 2017 (Cisco Visual Networking Index, 2013). Based on the growth, an organization's wireless network will realize increased utilization and load across the network. As typical in high-density wireless networks, the number of user devices and required application throughput will exceed the available capacity of a traditional wireless network. Since wireless networks are a shared medium, users and access points must contend for airtime to transmit data. In order to provide a high-quality user experience while meeting application throughput and latency requirements, a high-density Wireless Local Area Network (WLAN) must not only provide adequate coverage but also provide sufficient capacity to serve all client devices (Nagy, 2012).

Today's employees are tech savvy and they demand the use of rich media, including mobile applications and video, which is contributing to the need for increased WLAN capacities. As more and more employees access an organization's network using next generation mobile devices, the wire networks will become obsolete. Wireless networks will eventually be the norm for enterprises, causing heavy network usage (Mehra, 2011). Many companies planned wireless networks for projected headcount growth, but the explosion of mobile devices doubled or tripled the endpoint connections without increasing headcount. Consequently, additional devices on the wireless network can degrade signal strength and throughput (Accudata systems, 2013).With the added data usage of rich media including High-Definition (HD) video conferencing and streaming applications, an organization's mobile network may not be able to control the amount of bandwidth that is required and used by these types of media. In addition, business-critical applications running on the network may become impacted as users continue to purchase the

latest mobile devices available and bring them to work before the device has been certified for interoperability by the IT department. Mobile devices being used for personal and work related-purposes will drive social and applications usage, impacting the efficiency of an enterprise's mobile network. Organizations need to provide robust, scalable mobile solutions as more users and employees are expecting to access the network via their mobile devices.

### *3.1.2 Bandwidth Overload*

Today there are hundreds of thousands of mobile applications that users are regularly accessing from their mobile devices. In an enterprise environment, there are five heavy-bandwidth applications that impact the WLAN infrastructure: Video & Web Conferencing, Cloud Storage, AirPrint and AirPlay, Audio & Video Streaming, and Virtual Desktops.

**Table 2 - Top five bandwidth-hungry mobile applications**

| Application type | Applications example | Application usage example |
|---|---|---|
| Video & Web Conferencing | GoToMeeting, Google+ Hangout, Cisco WebEx, Microsoft Lync and Skype. | Skype requires 4 Mbps for five-way conferencing, and WebEx requires doubles the bandwidth for a laptop versus an iPad |
| Cloud Storage | Dropbox, Box, iCloud and Google Drive | 5GB - Unlimited storage, unless default settings modified by user |
| AirPrint and AirPlay | AirPrint and AirPlay(Video, Music) | screen mirror requires about ~1 Mbps for each Apple device |
| Audio & Video Streaming | Spotify, Pandora, YouTube, Vimeo, Netflix | Each audio stream requires about 500 Kbps of Wi-Fi bandwidth, and each video stream up to 2 Mbps. |
| Virtual Desktops | Citrix XenDesktop and VMware View | Laptops and tablets that rely on these apps require a minimum of 1.5 Mbps bandwidth. |

| | | |
|---|---|---|
| | | Internet and office-based sessions require 150 Kbps bandwidth, while printing and standard video sessions require over 500 Kbps. |

*Source: Aruba Networks, 2013*

Application usage for video and web conferencing will include more WLAN bandwidth being consumed if users join a conference with their mobile devices that have a larger screen size. Consequently, this will require approximately 4 Mbps for a five-way conference via an application, such as Skype.

Common cloud storage utilization includes the "free 5GB" cloud backup solutions presented by applications such as Dropbox, Box, and iCloud. The Google Drive applications allow for 15GB from the free edition however for business or education accounts, 30GB of storage are available. The other applications mentioned also have higher storage options available, though at a price that's not free. With some free storage solutions available to users, organizations, particularly higher education institutions, have WLANs that are being impacted by the heavy usage of these applications' downloads/uploads. The impact to the bandwidth will degrade all other applications on the network. Theresa Lanowitz, founder of independent analyst firm Voke, said "most companies are testing their infrastructure in a silo, not in an integrated environment, therefore they have no way of making sure applications, backups and storage will meet a defined quality of service" (Gittlen, 2012).

Utilization of high bandwidth is also associated with Apple products, such as AirPrint and AirPlay. These applications utilize approximately 1 Mbps for each device (iPad, iPhone, MacBook) for video streaming. If an enterprise with 1000 users utilizes the video streaming

capability, the wireless LAN infrastructure will be greatly impacted. With a minimum of 1000 Mbps being used, the high use of bandwidth will result in poor application performance.

Another bandwidth-intensive application type is audio and video streaming that includes Spotify, Pandora, YouTube, Vimeo, and Netflix. According to the Aruba Networks study, these are the top two bandwidth consumers in higher education institutions, along with video streaming on the rise (Kozup, 2013). Streaming audio and video is probably the norm at most organizations and higher education institutions. An audio stream requires about 500 Kbps, while video can require up to 2 Mbps over the air. All of this streaming can use up a lot of bandwidth, especially if the mobile devices are not using the higher 802.11n Wi-Fi rates/speeds.

Enterprise use of virtual desktops (Citrix, VMware) over WLAN via tablets and laptops will present a challenge to the network, especially in a high density environment. Bandwidth requirements will vary depending on the type of traffic, such as Internet and office-based sessions, which may require about 150 Kbps, printing and standard video sessions may require over 500 Kbps, and laptops and tablets may require a minimum of 1.5 Mbps bandwidth per device.

Hence, as more users continue to access cloud-based services, virtual desktops, and voice and video over wireless networks, this will undoubtedly lead to bandwidth overload. Combined with the abundance of new mobile devices in the market today, organizations will face network challenges as these factors will put a heavy strain on traditional wireless network bandwidth.

Rob Shaughnessy, CTO of Circadence, a WAN optimization company said “in this BYOD era, a corporate wireless network that scales to 50 devices is no longer enough” (Furbush, 2012). He points out that the need for scaling should include thousands of endpoints. According

to Xirrus, a Wi-Fi technology company, there are network bandwidth performance problems because single Wi-Fi connections can only support fifteen to twenty devices; any more than that and the connection signal strength begins to deteriorate. Furthermore, Xirrus explains that if thirty people are sharing a single connection then each device is only getting a 1 Mbps connection, which is insufficient to do anything productive (Furbush, 2012).

With the profusion of mobile devices and applications readily available, users will continue to utilize their devices and bandwidth-intensive applications within an enterprise, thus putting a strain on network bandwidth which could cause major incidents with internal business applications. In addition, bandwidth overload could hinder user productivity because of sluggish application performance. An example of this includes a situation where users may have to run critical reports on their devices and send them to management, but may run into trouble as the network bandwidth can cause a delay for a period of time because some other users are streaming video or music on the Internet. This is a challenge to any organization because it does not allow anyone to be productive and work efficiently.

In a recent study conducted by Aruba Networks, a provider of next-generation access management, network infrastructure and mobility application solutions for mobile enterprise networks, found that wireless LANs are not 100% optimal. With over 200 users surveyed, 70% of them often complain about mobile application performance (Dondurmacioglu, 2013). Many of the users that complained about this issue had indicated that their experience with certain mobile applications was poor due to the high bandwidth requirements of those applications. A report from MobileFuture.org mentioned that smartphones generate thirty-five times more traffic compared to regular phones, and most of the traffic is on the wireless LAN (Lancos, 2012). Therefore, since most users carry smartphones and use bandwidth-hungry applications, this will

lead to a strain on the wireless network. In addition, when compared to other devices, tablets will be utilizing the most amount of bandwidth because of the size of the screen and the variety of applications that are used. Therefore, as screen size of devices increase, so does the amount of WLAN bandwidth being consumed.

## 3.2 Adequate Wireless Access

Deploying a large-scale WLAN will present challenges such as coverage, capacity, density, and security. With the high use of mobile devices within organizations, IT is challenged by the number of access points required to meet the demand. The WLAN technology has changed since organizations began adopting the first-generation WLAN. It was originally designed to be "standalone" and connect directly to the existing wired network. The independent wireless access points were intended to create a small wireless network that provided basic connectivity and coverage for data applications in public use areas. There were issues in managing the devices and scaling to a larger wireless network with this technology. Organizations needed to adopt the second-generation WLAN technology which was designed to provide broad coverage, yet operate parallel to the wired network.

The traditional "hub and spoke" architecture is based on Access Points (APs) that forward all traffic to the WLAN controller, which acts as the central management for network and security policies being enforced. An AP is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired Local Area Network (LAN). APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to (Webopedia, n.d.). The Wi-Fi Access

Points (APs) were expected to deliver moderate capacity and coverage for data applications to a large area for an organization's conference rooms, lobbies, and other high-traffic areas. Due to the newer mobile device standards and the introduction of high-performance 802.11n Wi-Fi technology, the network became exposed thus creating a bottle-neck and sending all traffic to a centralized controller. The hub and spoke architecture has reached its full maturity due to the increased use of media rich, real-time and bandwidth-hungry applications like video in the enterprise.

The wireless technology of 802.11n integrated within mobile devices has greatly increased data throughput. Since all traffic is forwarded to the controller, it negatively affects the network performance of applications such as video. 802.11n is an Institute of Electrical and Electronics Engineer (IEEE) industry standard for Wi-Fi wireless local network communications, ratified in 2009. It was designed to replace the older 802.11a, 802.11b, and 802.11g Wi-Fi technologies (Mitchell, n.d.). In theory 802.11n technology supports a maximum network bandwidth of up to 300 Mbps.

Corporate campuses and universities typically cover a wide area; with many buildings and outdoor spaces where Wi-Fi coverage would be desired. Typically a Wi-Fi AP radius coverage is about 100 – 200 feet. This means that an enterprise or campus may require multiple APs for ubiquitous coverage, which does not make it a cost-effective approach. In addition, each AP must be connected to the network backbone to have full coverage, and in some instances it might not be a feasible option due to the physical location of the APs. Another area of concern for a Wi-Fi network is capacity limitations. Legacy single radio APs supporting only the 802.1b/g Wi-Fi technology are often not upgradeable. This limits the number of available channels for coverage. The problem with legacy APs is that they operate independently of each

other in its coverage area, causing frequency and power level interferences with other APs nearby. Legacy APs are programmed and managed in a distributed manner instead of relying on a central point of intelligence. Since they operate in an independent manner, it is difficult to ensure coverage does not interfere with other APs within a given area. Legacy APs do not have the capacity to identify and eliminate interferences automatically, which can be costly to resolve.

Density requirements are another challenge for organizations/campuses with high-density areas, such as an auditorium or a town hall with 500 plus individuals that need network connectivity for their mobile devices. It is becoming the norm for individuals to use applications that stream data, voice, and video to collaborate with each other in the corporate environment. It is also becoming more common at universities, as instructors increase their use of multimedia in classrooms and rely on the network for access, testing, and other applications. Therefore, it is necessary to have a high-density wireless solution for today's legacy APs.

## 3.3 Mobile Security and Risks

The arrival of new mobile equipment is unquestionably adding complexity to security operations while also loosening some of the strict controls the IT departments had been able to apply in the past.

### *3.3.1 The Mobile Device and its Data*

#### 3.3.1.1 Device Diversity and Support

Traditionally within an organization, IT pre-determined a list of approved workplace devices, typically a standardized desktop, laptop, and perhaps even a small, standardized set of

mobile phones and smartphones. Employees were allowed to choose from among these devices only and were not permitted to stray from the approved device's list. However, the vast array of personal computing device choices available today can be overwhelming. Smartphones, tablets, laptops, netbooks, desktops, and sometimes all of the above, are amongst the device options employees have these days. In addition to the devices, within each category additional brands (iPhone vs. Android), software and operating system choices exist. Given so much complexity, it can be challenging for IT to support and secure mobile devices in a way that delivers a consistent end-user experience. Therefore, with these devices evolving so rapidly, IT has to approach the problem differently. IT organizations are not able to have the same level of support for each and every device that employees may bring to the workplace (Spain, 2013). This affects the management of the types of devices that connect to the enterprise network and different levels of security risks. In addition, multiple choices in the devices, OS platforms, and applications require companies to employ diverse technologies for appropriate and effective security of the devices and data as they may need to be treated, configured and secured differently.

#### 3.3.1.2 Potential Loss of Data

With employees accessing corporate data on their personal devices, one of largest challenges that employers face is ensuring the protection of the corporate data. If a laptop, or another company-provided asset, is used to access corporate data and applications, normally that asset is tightly controlled by IT and may be subjected to added restrictive usage policies. Employee-owned devices such as a tablet or smartphone are regularly being used for personal access and business applications. As users bring their mobile devices everywhere, this can lead to devices getting lost more often than PCs due to their smaller form. In fact, 1 in 20 users have lost a device or had one stolen that contained work-related data (CDW's TMM Solutions, 2013).

To make matters worse, majority of the mobile and tablet devices are not usually locked with a PIN or password, and those that do are secured with just a four-digit PIN, thus the protection for mobile devices is not robust (Phneah, 2013). According to a recent survey by a risk and compliance services company, Coal Fire, nearly half — 47 percent — of users reported they still have no passcode on their mobile device (no change from 2012) (Weber, 2013). This, along with no encryption, can lead to unauthorized users easily obtaining access to the device and snooping around a lost or stolen device to extract valuable data.

In addition, termination or an employee changing roles within the company can necessitate the termination of access to the corporate data on the personal device in a timely manner. The concern lies with the potential loss of data in such events because companies struggle with revoking or updating corporate access from the devices. Lack of access control can result in a delay for IT to remotely wipe some or all of the data (and applications) on the device, thus potentially risking the loss of valuable data. The use of devices between personal and work-related data and applications can complicate the issue of data wiping.

Surprisingly though, an organization will only be able to defend itself if it has a remote wiping capability implemented. According to a recent survey by a risk and compliance services company, Coal Fire, found that only 51 percent of the participating companies reported that they don't have remote wiping capabilities (Hetrick, 2012).

Another source for potential loss of data can be found on today's devices as majority of the smartphones include some form of removable media to store documents, photos, music or videos. A user may utilize a cable to transfer data to and from his/ her personal computer with the use of a removable memory, such as a SD card or USB storage. As some companies permit

the use of removable storage at work, this can increase the risk of access to specific, sometimes confidential, data on a removable media if that device is stolen or lost. Because devices and removable memory are not secured or configured appropriately, this can lead to potential data leakage or loss. The least serious consequence that can be hoped for when corporate data is accessed by unauthorized parties is bad press and /or embarrassment. However, unauthorized access of devices may result in more serious problems for the company, such as identity theft or industrial espionage. Additionally, many public companies operate within compliance and regulatory environments. For example, in financial firms, a lost device could mean violation of the Sarbanes-Oxley Act or the Gramm-Leach-Bliley Bill, which mandate strict controls over disclosure of financial information. For health care companies, just the potential for unauthorized access to patient data violates the Health Insurance Portability and Accountability Act (HIPAA). Violations can result in significant fines, lost business or even forced restructuring (BlackBerry, 2010).

In addition, for convenient data storage, the use of public cloud-based file sharing and storage services can become possible sources of leakage for confidential corporate data. Due to its convenient instant access, everyone, at some point, may have been guilty of saving corporate presentations or other files and documents in free public clouds such as Dropbox, Box.net, Carbonite, Google Drive, Mozy, SugarSync, YouSendIt and Apple's iCloud but 67 percent of organizations don't have a policy in place around public clouds and 80 percent haven't trained their employees in the correct use of these platforms (Athow, 2013).

Public clouds are not secure, and can leave data constantly vulnerable in the digital environment. According to Websense, an organization that provides cyber attack and data theft protection, most other organizations cannot track data effectively and often rely on third-party

services to do so or hope their employees strictly follow best practice guidelines. This means there is no effective method of measuring the additional risk exposure from the movement of data (Phneah, 2013).

Furthermore, public cloud environments are also often incompatible with the IT infrastructure, causing business processes to become disjointed, and employee productivity to slow down. IT departments are well aware of the threats associated with using public cloud environments but may not be mandating appropriate policies for work purposes (Athow, 2013).

### *3.3.2 Rising Security Threats*

#### 3.3.2.1 Viruses and Malware

Today, downloading and installing mobile applications can increase the productivity of workers because the rise of next-generation personal devices and their rich applications can provide access to valuable backend data such as bank accounts, corporate (organizational) intellectual property and personal health information. However, this has undoubtedly caught the attention of a wide range of attackers who are commonly targeting these devices for their own gains. The potential for viruses being introduced to a network through a personal device is a major concern. That is because these devices are used for personal activities which are more prone to malware since they tend to access a number of consumer sites that don't necessarily provide a high level of security (CDW's Explosion of BYOD, n.d.). When employees download and install mobile applications for their personal use, they allow unregulated third-party access to other sensitive, corporate information that may be stored on their devices (Phneah, 2013).

The use of these applications can introduce other security risks for wireless devices as they become new targets for malicious third parties seeking to compromise a device or a

corporate network. Users often install questionable applications that may be pre-infected with viruses, Trojans, worms and other malware that can be unknowingly loaded onto wireless devices. Malware and viruses on mobile devices can threaten information confidentiality, endangers system passwords, increases the risk of data loss or compromise and potentially infects the company network. For these reasons, there has been a marked increase in mobile malware, which rose 155 percent in 2011 (Johnson, 2012).

#### 3.3.2.2 Default Bluetooth Connections

Bluetooth® is a standard for short-range wireless technology that enables devices such as laptops, smartphones, hands-free car kits or headsets to communicate with each other over a short range (approximately 10m) (BlackBerry, 2010). Although, in the past, a high profile security concern relating to Bluetooth was “Blue-jacking”, the bigger security issue today is the default factory settings of the new Bluetooth-enabled devices. Many Bluetooth devices are shipped with security disabled and default to “Always Discoverable.” They may also use short standard PINs such as “0000,” making it easy for malicious users to find and pair with a device and potentially intercept the flow of data. Furthermore, the malicious user may even gain access to core device functionality, such as voice, data and messaging (BlackBerry, 2010).

Without the appropriate security measures in place, hackers can connect and download data without the user’s knowledge, as well as access data traffic as it is being transmitted between the connected wireless devices. In addition, a similar concern relates to the mobile devices having the capability to enable a standard WLAN. This means that if an authenticated device has other devices tethered to it through an ad hoc WLAN, it may be possible for non-

authenticated devices and users to gain access to the corporate network by connecting through the authenticated device. For example, unauthorized access can occur when tethering a laptop over Bluetooth through a smartphone. The challenge for IT is how to permit the growing number of devices and capabilities to be used, while still maintaining the control to enforce policies, such as automatically disabling an ad hoc WLAN function on an authorized connected device (Anderson, 2013).

### *3.3.3 Lack of Comprehensive Mobility Policies*

Though the practice of BYOD is becoming widespread across American businesses, many organizations are still unprepared to handle the challenges presented by this shift. One of these challenges includes not having a formal mobility policy in place that can provide guidance for employees to follow when it comes to using their personal devices for work purposes. A survey conducted in 2012 by Coalfire Systems, a IT Governance, Risk and Compliance firm, found that out of 400 individuals from a variety of different industries (not affiliated with IT) across North America, more than half of the 84 percent of respondents, who use the same mobile device for personal use and work, reported their companies have no mobile device usage policy set up (Weber, 2012). This is a serious concern because companies don't necessarily own the smartphones and tablets that are being used by their employees for work functions, and thus they cannot control the flow of data among these personal devices or the applications in use. This can be a difficult process however the risk associated with allowing employees to access sensitive information on their personal devices can become a huge causality for a business if it is damaged, lost or stolen.

Therefore, companies need to research and implement a wide range of policies, depending upon their industry and its regulations and the company's own explicit policies. Because of the mixing of personal and corporate data on the employee-owned devices for work, it is critical to outline policies up front and be sure to communicate these to employees in advance. IT organizations need to familiarize themselves with laws, including the Computer Fraud and Abuse Act, the Wiretap Act, and Communication Assistance for Law Enforcement Act (CALEA) (Anderson, 2013). Companies must become proactive by having appropriate security and education policies in place that protect company data on personal devices. Comprehensive mobility policies are important given the risks and challenges that come along with BYOD, and also because they will guide the employees in becoming aware of their responsibilities and of certain outcomes if anything unexpected occurs. For example, policies might require that users report device loss or theft within a certain time period, so that IT can intervene to disable access and delete corporate data. In addition, IT's right to take action in emergencies, such as the right to remotely erase the device if it is stolen, must also be made clear. By doing nothing, company security is at risk as employees will continue to access email and other potentially proprietary data on their mobile devices. With a policy in place, access to data is controlled, and productivity can be extended to these devices (Forbes, 2013).

#### 3.3.3.1 Employee Privacy vs. Corporate Liability

The blurring of personal and private information on employee-owned devices and applications has been increasing at workplaces because of BYOD, and as a consequence, it has been raising privacy and legal concerns. Many organizations do not fully understand the BYOD concept, and its consequences, as potential ethical and legal embattlement can arise if policies are not established, communicated and enforced. As an initial matter, many organizations fail to

clarify and specify what employees can expect regarding the privacy of their personal information or email messages on their devices when accessing the corporate network. With regards to data protection, the concern lies with ensuring that as employees bring devices to-and-from the workplace, confidential corporate data is adequately protected while remaining easily accessible. In addition, an important component of data protection which is often not addressed by BYOD strategies includes ensuring that information and records comply with privacy laws, the accountability acts (HIPAA) and Sarbanes-Oxley (SOX), as well as specific industry and regional privacy regulations (Athow, 2013).

Because devices do not always make a clear distinction between personal and work-related data and applications, the issue of data wiping can be complicated if the device becomes lost. There have been several legal challenges recently for cases involving an employer who remotely "wiped" an employee-owned device, including both the corporate and personal data it contained (Cisco Bring Your Own Device, 2013). Therefore, policies that cover conducting e-discovery on personal data, terminating access to corporate data, monitoring and wiping data on the phone if device is stolen or lost, violations/rights of the employee and employer, are key factors that need to be communicated to employees as it affects their access and privacy of the personal device. In addition, employers often fail to ensure the BYOD policy includes employee consent for employer access and monitoring of the device. This will help employers make it clear to their employees on what they're signing up for when they agree to a BYOD program.

# 4 Developing an Enterprise Mobile Strategy

With the explosion of mobile devices and applications used on enterprise networks, IT is dealing with the growing demands by employees to deliver improved productivity and efficiency

through mobile networks. Developing and implementing a mobile strategy to handle smartphones and other mobile devices, ensuring multi-operating system support, security measures, and prioritizing access control for all mobile devices on the network is a complex and essential process for any enterprise to enhance the network infrastructure to meet the needs of rising mobile use. In fact, analysts say that 35 to 50% of enterprises today are a mobile workforce, relying heavily on their mobile devices for voice, data, and video communications (Manire, 2012). Having the proper mobile network coverage and scalable capacity for an enterprise is essential for an efficient and productive workforce.

It is essential to have a WLAN design, plan, and implementation strategy for high-density environments such as a corporate campus or university. High-density wireless networks are considered to be environments where the number of client devices and required application throughput exceed the available capacity of a traditional "coverage-oriented" Wi-Fi network (Aerohive, 2012). A legacy Wi-Fi network that is designed to provide good coverage, signal strength and signal-to-noise ratio (SNR) throughout an area is not enough to provide high performance due to insufficient capacity. As mentioned before, Wi-Fi is a shared medium, in which clients and access points must contend with each other to transmit data. Since the link between client and APs are shared on a particular frequency, it is difficult to determine signal strength as an indication of link quality compared to a wired connection. It is essential to design based on capacity demands to distribute the load of clients and APs across the available network range. Besides the importance of coverage and signal strength, the Wi-Fi network of an enterprise must consider capacity, channel utilization, interference, frequency reuse, and regulatory requirements as necessary components to the mobile and wireless architecture. The objective of this strategy is to equip an enterprise with a mobile architecture that is highly

scalable, with improved performance and reliability base on distributed intelligence so the network can be optimized without compromising security, quality of service (QoS), or costs.

## 4.1 Network and wireless architecture

Every enterprise network environment may not be the same, but it should be essential for every organization's network to be scalable, reliable and manageable. It is necessary to provide a cost effective network solution that can scale to accommodate the bandwidth overload created by the multitude of mobile devices and bandwidth-hungry applications being utilized on the corporate network. The solution must be reliable and deliver adequate wireless performance for the enterprise. The enterprise network should be equipped with adequate access and reliability throughout the corporate building with built-in redundancies and failover systems set in place to provide a continuous service in case of outages. It is necessary for a network to be centrally managed because it helps reduce daily tasks such as firmware upgrades, network monitoring of unauthorized access, and applying network policies if remote sites were not centrally managed.

### *4.1.1 Traditional "Hub and Spoke" Vs. "Distributed Intelligence" Architecture*

The traditional hub-and-spoke architecture innovation was for routing traffic through, and enforcing security at the wireless controller; however, the controller is now becoming the bottleneck for throughput and security enforcement as throughput needs have increased (Communications Today, 2011). There will be a tradeoff in cost or quality of service (QoS) if an enterprise continues to use the traditional architecture. To provide higher QoS, the network would need additional wireless controllers and wired switches, thus greatly increasing costs. With high throughput that 802.11n brings, utilizing a traditional architecture becomes

impractical. If the enterprise decides not to add additional hardware due to costs, then QoS and user experience will be greatly reduced. It is essential for an enterprise network to evolve and adapt to meet the demands of increased bandwidth consumption, enhanced reliability to deliver applications such as video, and minimizing network bottlenecks.

To help optimize the enterprise network to support business mobility, an upgrade to the wireless architecture is essential. A distributed intelligence architecture is necessary, as it is equipped to maximize an enterprise network performance and traffic without compromising QoS for video and voice features, security, mobility or survivability, while at the same time minimizing both capital and operational expenditures for a lower total cost of ownership (TCO) (Communications Today, 2011). Key advantages are the reduced cost in network installation, maintenance, and continual operating needs. A key benefit of this architecture is the ability of APs to continue to function even if it loses communication with the controller. Another import feature is the ability to deploy APs in remote locations without the need for a local controller. APs would coordinate with each other to provide optimized routing and self-healing functionality and deliver high QoS for business critical applications. Since the APs are self-healing, if any one does happen to fail then the other APs automatically re-route the data.

Distributed networks, also known as “Mesh networks”, use a special routing technology in which the software adapts dynamically and routes data packets based on changes to the structure of the network. In standard routing technology, the routing of data packets is fixed in sending and receiving information. In other words, the AP routing relies on the controller to determine where to send data packets. To achieve intelligent routing on the network, new smart adaptive wireless APs are utilized to offload some of the intelligence and functionality of the WLAN controller. The smart APs have the intelligence of the controller such as providing

security and acting more responsive to the dynamic wireless network. The smart APs do not need to be wired to a switch since they connect wirelessly among themselves via 802.11 links. Essentially, distributed intelligence forms the network and optimizes routing of data without smart APs having to forward the traffic to the controller, therefore eliminating a bottleneck. Designed properly, this type of network will deliver high performance, reliability, and redundancy without the need for complex planning and site surveying of the network.

### *4.1.2 Advantages of Next-Generation Distributed Technology*

Ruckus Wireless, a pioneer in the wireless infrastructure market, enabling carriers and enterprises, provides a distributed network they call “Smart Wi-Fi” (Ruckus Wireless, n.d.). Their patented “Smart Wi-Fi” technology allows a smart AP to navigate wireless signals farther, faster, and more reliably. Utilizing intelligent wireless components, such as smart antenna arrays, routing software (Smart RF), and optimization software (SmartCast) will help enable a high performance WLAN for an enterprise.

Smart APs are equipped with smart antennas (adaptive array antennas) that enable high throughput in wireless networks. Smart antennas evaluate load on nodes to help with routing data packets to a new route, resulting in a more load balanced network. It’s capable of reducing interference and improving overall network throughput based on a smart routing algorithm (AntMesh). AntMesh is a distributed routing algorithm which incorporates smart ants to find high throughput paths with less interference and improved load balancing specifically designed for Wireless Mesh Networks (WMNs) (Bokhari, & Zaruba, 2012). The smart antenna array structure is made up of many directional antenna elements that can be selected individually or in combination to optimize each packet transmission. Essentially the elements can be selected to

focus transmit energy toward the receiver for improved throughput, or reject interference from the opposite direction, thus reducing interference.

The routing software controls the smart antenna array by intelligently adapting the environment and re-configuring the array to select the best antenna pattern. Antenna pattern for a WLAN is best described as how the antenna radiates energy out into space (or how it receives energy) (Cisco, 2007). In essence, the software enables a smart AP to avoid interference with other devices in real time using the adapting antenna configuration, thus increasing throughput. Furthermore, it allows for operating at maximum performance, highest data rates, and most efficient Radio Frequency (RF) channels with minimal retransmissions. The software enhances the performance, connectivity, and coverage allowing for a more reliable network.

Performance optimization software is another component for an enterprise WLAN. It adjusts fair air time usage among devices operating at different speeds. Airtime fairness is an advanced scheduling technique that ensures legacy Wi-Fi clients and underperforming 802.11n clients don't slow down the performance of faster 802.11n clients by taking too long to transmit (Ruckus Wireless, n.d.). Other capabilities include access to scheduling based on traffic type and/or client priorities, and allows for rate-limiting bandwidth per user to prevent any usage hogging. For example, a user that continually downloads or streams videos on the network. Rate-limiting feature is important because it prevents mobile devices from consuming excessive network bandwidth.

In regards to performance, when non-intelligent APs face interference from other devices, they drop data packets or lower the transmit data rate, essentially reducing system throughput. Smart APs have the ability to avoid the interference by finding an optimal signal

path that prevents packet loss while preserving higher transmission rates. If it fails to find a quality signal path, then integrated software will automatically help reroute when it detects a significant performance decrease in an AP.

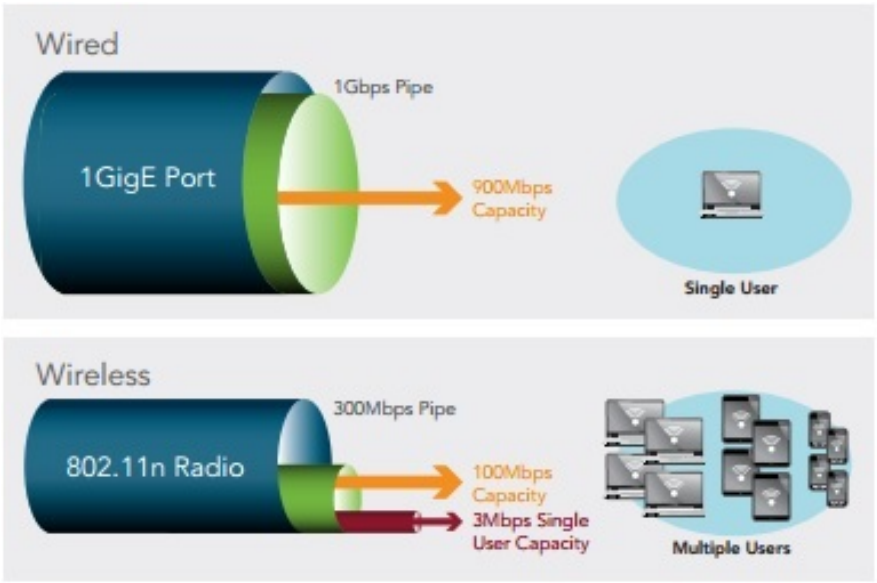
Distributed wireless networks have the reliability factor that is required for an enterprise to sustain consistent coverage without any interference or dropped connections. Smart AP antenna arrays provide reliability to the network by focusing transmit energy toward the intended recipient for the duration of a transmission. It is essentially similar to a concentrated beam from a flashlight where you can adjust the light pattern to have a narrow focus instead of a wide focus. This minimizes the probability of interference in the network, thereby allowing contiguous APs to attain higher performance levels.

Distributed wireless networks such as “Smart Wi-Fi” allow for simplified deployments and operations by automating key tasks such as design, configuration, optimization and maintenance of the enterprise network. An advantage of this technology includes minimal requirement for complex site surveys, RF design, and expert installers. Another key advantage is self-optimization in which wireless performance is barely affected by the physical positioning unlike, non-intelligent APs which would require manual intervention. The technology provides an overview of the network topology on a floor plan map view for continuing operations. This helps administrators gain a better understanding of issues such as single points of failure to bottlenecks in the network. There are also reports and logs that capture network usage and other information required for continuing operations and maintenance.

### *4.1.3 Optimizing the Enterprise Network to Support Business Mobility*

While most wireless architectures may be sufficient in meeting the current mobility needs, organizations should consider exploring optimization plans for enterprise WLANs because it can enhance network performance. Wired networks, which are different from WLANs, provide high throughput without much overhead, where users can achieve hundreds of Megabits per second (Mbps) from a Gigabit network. In contrast, WLANs, unfortunately, use a shared medium and are typically provisioned with less than 5% of the capacity per user compared to the wired network (Xirrus, 2013). They require greater overhead to handle the shared medium and retain compatibility with earlier wireless technologies (802.11a/b/g). An example of bandwidth difference between wired and wireless networks can be seen in figure 2. Essentially a standard wired network utilizes 1 Gigabit per second (Gbps) with very little overhead, resulting in a high throughput per user. Unfortunately, a standard 802.11n wireless network capacity is rated at 300 Mbps with a great amount of overhead, resulting in a lower throughput per user.

**Figure 2 - Bandwidth Differences between Wired and Wireless Networks**




Source: Xirrus, 2013

Under these conditions, it is essential that the wireless infrastructure be optimized to provide reliable performance even under heavy network load. Optimizing the wireless network is necessary for business-critical applications now and into the future for an enterprise.

#### 4.1.3.1 Focusing on Key Areas for Optimization

Organizations must consider a wireless infrastructure that accommodates user access to the network without any interruptions. When authorized users are in range of the wireless network, the infrastructure must authenticate and connect them regardless of the number and type of devices that they use. The network must allow new employees and guests quick access. It must also allow employee devices to access critical business applications and data without sacrificing security. With security in mind, anonymous users must be isolated from the business traffic; instead they should have access to the guest network. Furthermore, guest or free network access should have performance limit policies set so that the network does not degrade. It is

essential for organizations to select a proper access manager solution that allows employee devices to be authenticated and identified seamlessly once given access to the network.

Application optimization is another key area that is essential for the organization to focus because business-critical applications performance degrades due to increases in bandwidth use from the growing number of wireless devices and applications from those devices. In a recent survey, 40% out of 1,200 IT professionals and 1,200 workers said they had already seen degraded network performance due to BYOD programs and mobile devices (Hill, 2013). Therefore application traffic control technology is required to guarantee that business-critical applications perform without any network degradation.

Enterprise applications such as file sharing, e-mail, and collaboration must be prioritized based on network usage. An example is providing collaboration tools such as WebEx and LiveMeeting the highest network priority because they involve real-time video and audio use. Application control is feature integrated into smart APs to reduce network traffic. It uses advanced deep packet inspection (DPI) technology to analyze application traffic in detail to not only identify the application (e.g. Facebook), but also the specific usage (e.g. a FarmVille game). DPI technology provides more insight into traffic usage patterns, allowing them to formulate policy enforcement rules that will improve and optimize network performance (Developing Solutions, n.d.). With application control, non-critical traffic is limited or denied before it can congest the enterprise infrastructure. With application control, business applications can be prioritized, inappropriate activities can be blocked, and recreational applications can be rate-limited.

### *4.1.4 Network Management*

An organization should determine whether a local network management system (NMS) is required or if a cloud-based system is a more practical solution. A local NMS approach is appropriate in high-density environments such as conferences, events and trade shows to ensure fast and responsive network management operations. It works well in large enterprise environments with local IT staff, but does not suit as well for smaller organizations that outsource more IT resources. A cloud-based approach was introduced to deal with the growth of BYOD in the enterprise. Chris DePuy, an analyst at Dell'Oro Group explains the need for cloud management because "BYOD has dramatically increased the complexity in managing WLAN infrastructure" (Rubens, 2013).

A NMS is an application or set of applications that lets network administrators manage a network's independent components within a larger network management framework (Janssen, n.d.). It is used to monitor both software and hardware components in a network. The system assists in network discovery, device monitoring, performance analysis, device management, and intelligent notifications.

Network discovery assists in identifying devices and changes to software in the devices on the network. Device discovery is an important part of inventory and software management, as it provides a detailed inventory of hardware models, installed components, and software images. This will help organizations complete tasks such as software and hardware maintenance. Changes in software and hardware must be tracked to assist in the analysis phase when hardware and software changes are required.

Device monitoring assists in determining the health of network components and the extent to which their performance matches capacity plans and enterprise service-level

agreements (SLAs). Monitoring devices provides performance metrics on Central Processing Unit (CPU) utilization, buffer allocation, and memory allocation. Network performance is dependent on the buffer availability in the devices. Monitoring device-level performance is essential in optimizing the performance of these network protocols.

Performance analysis assists in tracking bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other devices. Administrators need a detailed view of traffic in the network to analyze, monitor, and troubleshoot devices that put strain on network resources.

Network device management assists in ensuring proper functioning and security of network devices. It is used to ensure that devices such as routers and switches have the latest configuration data and that network firewalls are functioning properly. Intelligent notifications assist in sending modified alerts that will respond to specific network scenarios by calling, emailing, or texting administrators about it. Possible scenarios can include battery or fan failure in a device that needs attention. The purpose for organizations to use this is to detect, isolate, notify, and correct any issues on the network.

#### 4.1.4.1 Network Access Control (NAC)

Mobile network security is a complex task where network information must be protected from the growing number of mobile devices. It requires attentiveness as well as solutions that will improve security without affecting productivity. Organizations must take proactive measures to secure network access, sensitive data, applications, and services, and to enable device authentication as an essential step in securing the mobile network.

Network access control (NAC) solutions are designed to be aware of every device on the network so as to help make decisions about which devices are allowed to communicate with everything else (Quellette, & Thomas, 2011). NAC can also determine if the device is equipped with the latest patches, updates, and policies. A possible scenario of access control is for the NAC solution is configuring it to inspect devices that must have the latest anti-virus software. If any device is not up-to-date, then the device would be quarantined and restricted from the network until an update had been applied. NACs provide an effective way to manage the risk of employee-owned devices. It allows organizations to control which devices can access each level of the organization's internal network. Basic authentication can be enabled for users connecting their devices to the network, while advance authentication methods are required for users that access encrypted email sessions or critical applications.

#### 4.1.4.2 Best Practices to Consider

The network infrastructure is an important part of IT as a whole, but it is just a piece in the entire scope of IT management. For that reason, network management practices and the tools that support them must align with IT management systems, processes, and initiatives. Best practices help administrators get a better perspective of IT management as a whole instead of the daily work tasks that are assigned to them. The following are network management best practices for an organization to consider.

Integrating management functions is necessary for any organization to follow, because it helps with unifying changes so that accuracy of the network is not impacted. The best levels of management awareness and control exist when management tools used for various management functions are integrated. This means when there are device changes or performance degradation

on the network, it is wise to use a unified management system that supports multiple functions such as configuration management, availability, and performance monitoring for troubleshooting. This results in an improved and efficient enterprise network.

Multi-vendor support is necessary to organizations, because administrators usually don't manage products from one vendor. More than likely a diverse set of products are utilized and finding a management suite that can support various vendors will help reduce the number of tools required, eliminating the need for learning and maintaining various management tools, thus improving operational responsiveness and efficiency. The management suite must support devices from multiple vendors and support functional tasks such as configuration, monitoring, and troubleshooting.

Automation is necessary for any organization that wants to take redundant tasks away from administrators so they can focus on other important tasks. Changes in networks are rapid, with advances in new technologies and devices; administrators need to leverage automation to keep up. Organizations should look into network management tools and technologies to help automate tasks. With auto-discovery technology, devices being managed are recognized and have a feature to provide incremental updates to devices and configurations. Basic tasks can be setup to run based on a date and time scenario or triggered by an event. Leveraging automation will help keep pace with changes, increasing productivity and accuracy of tasks.

Having a unified policy management system is necessary for organizations, to provide needed security and levels of service to the end-user. It can be challenging if the security and network planning are independent of each other. This means various tools and systems must align with each other to achieve consistent levels of security and service. If this is the case, then

it will require collaboration between the operations, networking, and security teams to define implement, and enforce the policies. Organizations should utilize a tool that will unite security and usage policy definition with application and network monitoring needs. This will assure that policy goals are met, while providing administrators with an analysis of the issues.

Utilizing a proactive monitoring system is necessary for organizations, because it provides administrators with the ability to determine the health of the network so they can better understand the business impact. Utilizing a dashboard that presents the baseline features of the network helps administrators see any abnormal activities. This tools present preventative actions that reduce the impact on the business.

Communication and collaboration are an essential practice for any organization. The ability to translate the network details to other teams outside of IT is crucial, because they will not fully understand their impact on the network and the business. Providing metrics and reporting tools for other teams will reduce confusion on what is impacting the business. Network managers need to share and collaborate on the network health and status with other teams so the business can be proactive instead of reactive to make important decisions.

## 4.2 Securing the Mobile Device and its Data

### *4.2.1 Enterprise Mobility Management (EMM)*

The BYOD trend has forced business leaders, CIOs and IT professionals to reexamine their approach of the smartphone and tablet use within their organizations. The growth and acceptance of personal mobile devices in the workplace is driving increased user expectations for

access to their organization's applications, data, and content. Organizations must ensure all confidential data and content are protected. This requirement makes mobile security a key consideration for any corporate mobility plan. With the increasing concerns related to security, management and network controls, organizations should begin considering a solution that can unify all of the management and security capabilities under one platform. This platform is referred to as enterprise mobility management (EMM). EMM involves some combination of mobile device management (MDM) and mobile application management (MAM) technologies that can work together to enable secure enterprise mobility.

In the growing mobile environment, the traditional form of management, mobile device management (MDM), is still a key component to network and device security because it is evolving and providing capabilities far beyond its original intentions. However, it is not the only piece to the puzzle. Mobile application management (MAM) is the other management and security function that is maturing and becoming a necessity as well due to its continual improvement to device capabilities and the application of those capabilities into the workplace (Adamson, 2012). Both of these approaches are viable, and at least parts of each are required for successful enterprise mobility management (Mathias, 2012).

However, there is not one specific solution or strategy when it comes to every individual company. These two technologies both address specific concerns but do not provide complete solutions to all of the problems that enterprise mobility can cause or exacerbate. That is why it is very important to really focus on the organization’s specific security strategy and mobility objectives. By determining what is most important to the organization, the right solution, perhaps one with a more singular focus on MDM or MAM may stick out to be practical. Understanding what is truly needed to offer the best mobile security for the organization will help the IT

professional make the ideal decision. With these approaches combined or not, organizations must keep in mind that mobility is more about enabling mobile workers by giving them the tools they need to do their jobs better.

#### 4.2.1.1 Mobile Device Management (MDM)

Standardizing mobile platform can potentially reduce IT complexity but with the proliferation of the devices being used by employees today, it is not likely to happen in the near future. The platform diversity only exacerbates the resource issue for the IT departments. Therefore, many IT professionals are evaluating mobile device management (MDM) systems to help them manage the variety of devices entering the workplaces. Whether the mobile device is employee-owned or company-owned, if it has access to an organization's network and resources, it requires a MDM solution installed (CDW's TMM Solutions, 2013). While most enterprises recognize the need for MDM in the world of mobile workplace, many have not yet deployed it. In a survey of over 300 IT executives conducted by Computerworld, a full one-third said they had no MDM policies or technology in place (Bort, 2012).

Nonetheless, MDM is in a class of software that was developed to cope with the problems raised by BYOD, and the proliferation of portable computers in businesses generally (McLellan, 2013). It lets organizations control the employee-owned devices in the same way they control legacy systems, such as PCs and laptops. MDM is intended to provide centralized security and management of mobile devices in order to protect corporate data stored on the devices, and data that these devices have access to (Sophos, 2013). Essentially, it allows for remote visibility and control over smartphones and other handheld devices that are carried by employees.

- *MDM checklist of features and options*

MDM allows administrators to enroll and manage assets on the network, configure settings, remotely locate and wipe devices, distribute software, track usage and enforce corporate policies relating to passwords and other security measures, across all operating systems including Macs/iOS, Android, and BlackBerry. However, because the term MDM applies to a diverse collection of products, the first step for an organization is to define precisely what an MDM system can do for its mobile workforce. This process should include checking off which of the available features and options (See table 3) that are available in MDM are suitable for the organization:

- Mobile asset inventory: In order for devices to be managed, MDM must maintain a list of devices that need to be managed. This is where a mobile asset inventory needs to be created by taking into account the various options available to help an organization determine what the inventory should include and how it will be maintained.
- Mobile device provisioning: Because managing a mobile device through its lifecycle begins with activation and provisioning, it is essential for an organization to determine how each new device will become an authorized, capable member of the handheld workforce. By requiring enrollment, IT can allow mobile flexibility for the employees and gain visibility into who and what is accessing the corporate resources all while enforcing the mobile policies (CDW's TMM Solutions, 2013).
- Mobile data protection: MDM can help preserve and protect mobile data that might contain confidential corporate data. In addition, MDM can assist IT to become aware of how the employees access, transfer and collaborate on corporate content. Whether

documents are sent to the users by email or via cloud-based file sharing, MDM can be considered as an encryption solution that encrypts data before it is uploaded to a cloud-based file share, and still allows mobile devices with the right credentials to interact with the content stored in the cloud (Sophos, 2013).

- Mobile software distribution: MDM can go beyond device inventory and configuration, providing tools that deliver and update mobile applications.
- Mobile security management: On handhelds, device and security management tend to converge. Many MDMs offer basic security features that are missing from mobile OSs or related to device tasks such as the ability to "remote wipe" lost devices which is critical as it allows the IT administrator to locate, lock and/or delete corporate data on a device. MDM reduces IT's work load but also enhances efficiency, users can be empowered to locate, lock and wipe their own devices if needed via a self-service portal. Because the users are the first to know if his or her device is lost or stolen, they can take immediate action.
- Monitoring and help desk support: MDM can help reduce maintenance and support costs.

**Table 3 - MDM Features and Options**

| MDM Options | Features available |
|---|---|
| Mobile asset inventory | • Device inventory<br>• Inventory classification<br>• Inventory maintenance<br>• Physical tracking<br>• Database integration |
| Mobile device provisioning | • Supported platforms<br>• Device registration/ enrollment<br>• Agent activation<br>• Device configuration |

| | |
|---|---|
| Mobile data protection | • Data encryption<br>• Backup/restore<br>• Data tracking |
| Mobile software distribution | • Software packages<br>• Application distribution<br>• Mobile optimizations<br>• Change control |
| Mobile security management | • User authentication<br>• Password policy enforcement<br>• Remote device wipe<br>• White/black lists and device restrictions<br>• Secure communication |
| Monitoring and help desk support | • Self-help/ diagnostics<br>• Remote control<br>• Audit and compliance<br>• Activity reports<br>• Alert messages |

(Phifer, 2013)

- *MDM Delivery*

MDM was traditionally being delivered as on-premises software which means it is available for installation on the enterprise server. However, now it is also available as a cloud service. Increasingly, vendors that provide MDM will offer both kinds of software as companies may want a mix of cloud and on-premises software.

MDM is fundamentally a security application and it is a concern on how it is delivered because software installed on a server allows users to enable data encryption on all supported devices, whereas cloud services do not always provide that level of protection. With on-premises software, data can be backed up to the corporate data center behind the security firewall, or over a local network when the device is being used in the office. That can be a safer, more secure choice for companies than backing up data via the cloud, especially in highly regulated industries, where using cloud services may violate regulations (McLellan, 2013).

The cloud, nevertheless, is the wave of the future, and not just for MDM but for all kinds of enterprise software. With a cloud service MDM, companies can react more quickly as the mobile market is changing rapidly, and each mobile operating system vendor is pushing out system updates at their own schedule. When MDM solutions are updated to support devices across the different platforms, those updates are pushed out to all of their users practically instantly.

On the other hand, if the cloud service provider goes down, so does its software. Preventing that requires running the software in multiple locations, which increases costs (McLellan, 2013). Nonetheless, MDM software is necessary in the here and now for organizations that want to encourage more productivity and provide an appropriate level of security.

#### 4.2.1.2 Mobile Application Management (MAM)

Employers that embrace BYOD by implementing MDM for enrolling and configuring devices have addressed fundamental mobility concerns. This enables employers to safely permit employee devices to access corporate email or Web portals, but employees want to do more than just that. They carry powerful mobile devices that have the CPU, storage and displays to run real business applications. Therefore, to address this potential, mobile application management (MAM) is introduced.

With MAM, the creation, deployment and management of internally- and commercially-available applications used in business settings on personal mobile devices can be simplified and secured (Phneah, 2013). Compared to the capabilities provided by MDM, MAM is concerned with the applications that run on the device and not the device itself. Thus, this eliminates the

likeliness of compromising the user experience at the device level.The software distributes and updates applications based on company need or recommendation, configures application settings, tracks versions of the installed applications, uninstalls applications when an employee leaves the company, and reports on application use. It can also install corporate applications even on devices not owned by the company.

- *Application Management*

MAM provides control over the applications that employees run on their mobile devices. This is essential as a rogue program downloaded from a mobile OS's native application store could potentially, and easily, compromise a corporate network. Although it can't remove user-installed public applications, MAM tools can work with MDM to respond to potential non-compliance. Together, MAM and MDM can change a device's settings to prevent access to the corporate email or network (Phifer, 2012).

In addition, MAM tools can help employers manage business use of public applications that can be downloaded from the Apple App Store and Google Play. While organizations are really just getting started with developing their own private applications, MAM can be customized to ideally house these applications where all approved applications can be made available or deployed securely to particular users or groups. Role-based access control allows organizations to ensure that employees have access to the applications they need. Employers may insist that some or all enrolled/registered devices should have mandatory mobile security measures, such as virtual private network (VPN) clients, anti-malware, secure browsers, and virtual desktop clients, installed on them. Whenever an update to an enterprise application is released, MAM tools can inventory all devices to identify which ones are running old software

and then initiate silent over-the-air policy-driven updates to those devices. Using MAM to automate application installation and updates can reduce the costs associated with letting the help desk troubleshoot incorrectly configured or poorly written public apps. Finally, MAM can help disable enterprise applications on non-compliant devices, former employees' devices, devices that are being retired, and lost or stolen devices by removing the device from the management control. These basic MAM capabilities can help put users' devices to better use (Phifer, 2012).

While so many applications are available today and more are being developed each day, implementing a blacklist of applications, that are deemed insecure or damaging in some way to employee productivity, can increase mobile application management and security (McLellan, 2013).

- *Application Wrapping*

A more advanced, and increasingly important, feature is application-specific security via containerization (also known as application-wrapping or application-sandboxing) where important applications, like corporate email, get individual secure connections to the enterprise network (McLellan, 2013). This approach, as the name implies, is applied at the application level, wrapping corporate applications and data, but not wrapping Facebook or Roku. It provides a high level of administrative control while still offering appropriate user experience for all mobile applications, both with the wrapped and unwrapped content. Security for mission-critical applications can take advantage of this feature which encrypts transmissions so that users can safely access the data they need to do their jobs. That is because when this feature executes, inside information cannot go out, and outside information cannot come in. Therefore, this prevents other applications on the mobile device from accessing the organization’s sensitive

data. It also prevents the sensitive data from “leaking” into other parts of the mobile device that are not protected by the MAM software. Separating corporate and personal data on the mobile devices seems to be a popular new way to address the security risks posed by mobile applications.

### *4.2.2 Mobile Virtual Desktop Infrastructure (VDI)*

Although virtualization has had a huge impact in datacenters and has long been used to run multiple OSs on desktop systems, there have been concerns with it being utilized in the mobile space. However, as mobile devices become even more functional in terms of CPU and GPU power, storage capacity and connectivity, the idea of creating virtualized mobile space has been explored. Today, IT professionals can create a secure, managed, virtualized space on the personal mobile device in which all business-related activities occur. This technology allows IT to send the corporate standard image to all those devices easily and without rewriting applications or supporting new front-ends. It is completely isolated from the device's native environment, which remains the user's personal domain. Corporate and personal digital assets are kept separate from where IT controls corporate digital assets, while end users manage and maintain their personal applications and data.

Forrester Research predicts in its 2013 "Mobile Security Predictions" report that "on-demand mobile virtualization will overtake mobile-device management" as a core technology that IT professionals will turn to as a way "to segregate business content and data from the personal environment" in mobile devices (Messmer, 2013).

The mobile VDI technology refers to the infrastructure that provides a virtual desktop of sorts to mobile devices, such as notebooks, tablets and smartphones, regardless of which mobile device platform is used. The mobile VDI solution provides a thin client experience that is intended to be consistent across different types of devices, except for those physical characteristics that are device-specific (such as screen size and input method). Mobile VDI has two basic client architectures (Mobile VDI, 2013):

- *Client-based mobile VDI*
    - Typically, a mobile VDI client application is installed on each mobile device. This application creates a VDI session between the mobile device and the organization's computing infrastructure. The VDI session allows the mobile device to access various applications and data through a virtualized interface.
- *Browser-based mobile VDI*
    - An alternative architecture uses a web browser (generally, one that supports HTML 5) to access a web-based mobile VDI client. With this architecture, it's unnecessary to install a mobile VDI client application on the mobile device itself, and it is assumed that the mobile device already has a web browser. Regardless of the client architecture, mobile VDI works by giving the mobile user an image of a virtual desktop. This means that the data and applications stay at the organization's facilities and are not present on the mobile device. Only a snapshot of the virtual desktop is transmitted to the user's mobile device. The user's interactions with this snapshot, such as entering data into dialog boxes and clicking on menu options, are transferred back to the VDI infrastructure and converted into their application equivalents.

Employees can connect to the network 24/7 with the device of their choice—laptop, tablet or smartphone—regardless of whether they are using a Windows, Mac OS, Linux, iOS or Android platform. The networks that authenticate BYOD devices can be isolated so users access only the data and applications they should. Isolation minimizes the risk of malware coming onto the network, so IT does not need to worry if users have the latest versions of firmware or other software on their personal devices.

In addition, mobile VDIs can reduce the need for client software on mobile devices because both these thin client options provide a significant benefit compared with the thick client alternative, such as the MAM sandbox/ wrapping. A thick client requires installing many client applications on each mobile device, perhaps one client for each application that needs to be accessed through BYOD (and for more complex applications, multiple clients). Minimizing the installation of client software provides multiple benefits. Obviously, it reduces the amount of technical support involved in installing the software, but it also reduces related maintenance concerns, such as patching and security configuration. It provides a more consistent experience for users, which should cut technical problems and associated support costs. And it also improves security by reducing the number of pieces of potentially vulnerable software being run on the mobile device (Mobile VDI, 2013).

Also, by centralizing access to many applications through a single client interface, mobile VDI technologies can enable single sign-on capabilities for these applications. The mobile VDI technology requires users to authenticate, and this authentication can be integrated with enterprise single sign-on technologies (Mobile VDI, 2013).

However, there are quite a few major caveats that include a high probability that some applications running on the mobile VDI will not display well or be unable to function at all on a smartphone or tablet with these factors:

- over any VDI interface;
- be greatly slower on some older, underpowered devices;
- be greatly slower over slow links;
- without a keyboard, or;
- without a traditional input device (mouse, track pad or pointer).

### *4.2.3 Corporate Data Protection*

These days, the global growth in 3G/4G networks, public Wi-Fi deployments (Hotspots), and home and business Wi-Fi can provide a reliable, seamless wireless network for popular data applications such as email and Web browsers. Unfortunately, much of the growth in mobile data usage is not secure. Employees using their personal devices for work purposes are frequently connecting to unsecured public networks to exchange sensitive corporate email and access strategic business applications. Therefore, since most wireless networks that employees connect to reside outside of the corporate environment, organizations need to suppose that no innate data protection exists. An enterprise's most important information assets can be transmitted over any wireless network, thus making protection of the sensitive data in transit a critical task for IT professionals.

#### 4.2.3.1 Securing Communications

The ability to securely and effortlessly manage any data and applications specific to the enterprise on the employee-owned devices is via a centralized solution, such as EMM or Mobile VDI. To assess the strength of a wireless solution's security, an organization must measure its ability to maintain confidentiality, integrity and authenticity of the data residing on the device and through its journey across the wireless network, from personal device to the enterprise network (BlackBerry, 2010).

- Confidentiality

To provide data confidentiality via a wireless solution, data encryption and an encrypted tunnel over which the data is transmitted should be used. Data encryption uses a secret key to encode information in a manner that can only be decoded and read by the parties for which it is intended. Most modern cryptography solutions are based on the Advanced Encryption Standard (AES). AES is required by U.S. government agencies and is considered secure enough to be used in sensitive military applications. An encrypted tunnel is setup when a Hypertext Transfer Protocol (HTTP) connection is established over Secure Socket Layer/Transport Layer Security (SSL/TLS). This provides additional authentication and security if wireless devices are accessing servers on the Internet. Many secure internet transactions, such as online banking, already require support for Hypertext Transfer Protocol Secure (HTTPS) (BlackBerry, 2010).

- Authentication

With the use of authentication the recipient is able to identify the sender and trust that the sender actually sent the message. Authentication can be accomplished through the use of a

cryptographic shared key system, which requires that an authenticating component (such as a server) and a requesting component (such as a wireless device) both recognize a secret key. When a connection is attempted, the server sends the secret key, and the wireless device either accepts or rejects the key. Before encrypting the data to be transmitted, the wireless device checks with the back-end system to determine if the keys match. For successful data transmission to occur, the keys on the server and the wireless device must match. If the keys do not match, the server and the wireless device cannot send data between them. To prevent unauthorized users from pretending to be a legitimate device and accessing the network, a device should authenticate itself to the network and enterprise systems. On the other hand, the server should authenticate itself to the mobile device to prevent unauthorized users from pretending to be a corporate server (BlackBerry, 2010).

- Integrity

Data integrity refers to the validity of the transmitted data (for instance, whether the data has undergone any changes or modification in transit). By using various prevention and detection mechanisms, the trustworthiness of the transmitted data can be determined. If a message contains encrypted data, failure will occur automatically if the message format is unrecognized in the decryption process. In addition, failure will also occur if the message received is encrypted using the wrong encryption key or if the data has been altered during transit. The selected wireless solution should automatically eliminate changed packets of data to ensure that malicious or false data has not replaced the valid data (BlackBerry, 2010).

#### 4.2.3.2 Data Loss Prevention (DLP)

Data loss prevention (DLP) software, which is also known as data leakage protection solution, has been around for years and is quickly evolving to become more effective in today's workplace setting that now includes an influx of mobile devices. DLP security software helps monitor the use of organizational data on personal devices in order to protect it from possible leakage unsecured or unauthorized locations. It can help monitor three types of information (CDW's Take Security to Go Report, 2012):

- Stored information
- Transmitted information
- Information manipulated by actions on each device

Many DLP offerings are being expanded to address BYOD's unique security concerns. This typically involves expanding the solution architecture to include specific mobile device brands or rolling out a new solution to provide DLP oversight to mobile devices. As a security measure, communications to and from the personal mobile devices should be proxy-based, and the mobile device should not communicate directly with back-end systems. Network-based DLP software deployed at the proxy server can monitor the unencrypted communications between the two encrypted segments, and therefore stop sensitive information from being transported against policy (Scarfone, 2013).

All communications should go through a host which resides in the Demilitarized Zone (DMZ). In addition, all data at rest or transmitted should be protected by end-to-end encryption, preferably using 3DES 192-bit encryption on the server and AES 256-bit on the device or when sent over the air (Goldberg, 2013). From an end-point perspective, many

organizations have already deployed endpoint security protection suites to their desktops, notebooks and mobile devices. These suites, which provide an integrated defense-in-depth approach to endpoint security, often include an endpoint-based DLP capability. Once this is properly configured and activated, the suite will examine all activity within the endpoint before encryption is employed. Endpoint-based DLP can even detect forms of data leakage that network-based DLP can't spot, such as transferring sensitive data to USB flash drives. As a result, endpoint-based DLP may offer more effective detection than a network-based solution (Scarfone, 2013).

### *4.2.4 Additional Security Controls*

#### 4.2.4.1 User Authentication on Devices

On mobile devices, the key to protecting stored information is preventing access at the device level. In cases where physical access cannot always be prevented, other measures must be considered as well. First, all devices, whether corporate-provided or employee-owned, should be password protected. Although, at times when password authentication isn't always enough for certain organizations, the use of smart cards, biometrics or other similar mechanisms are options that can easily provide stronger protection against unwanted access to mobile devices Multiple factor authentication increases security by ensuring that access to the device requires not only something the user knows (the mobile device password), but also something the user has (for example, a smart card) or something the user "is" (for example, the user's fingerprint) that is unique only to the user (BlackBerry, 2010).

#### 4.2.4.2 Bluetooth Connections

The bigger security issues today are the factory settings of the new Bluetooth-enabled devices. One way to maintain security is each time when a user attempts a connection via Bluetooth, the device should be configured to alert the user and require confirmation that it is connecting to a trusted device using Bluetooth technology. In addition, all data traffic that is transmitted between connected wireless devices should be encrypted as this can prevent hackers from connecting and downloading data without user knowledge, as well as access data traffic as it is being transmitted. In certain cases, some companies allow Bluetooth headsets for voice but not Bluetooth access for data from laptops or other mobile devices which is the most effective in securing Bluetooth connections.

#### 4.2.4.3 Removable Media

To prevent an unauthorized user from accessing removable media, such as SD card or USB storage, and extracting valuable data, the device should enable encryption of data and any removable data stores. Although, some companies will permit the use of removable storage, others may find this unacceptable and mandate its disability for work purposes because of the regulatory and legal issues surrounding sensitive data. If an organization does allow removable media, the data on the removable media should be encrypted as securely as the data stored on the device (BlackBerry, 2010).

#### 4.2.4.4 Viruses and Malware

Employers should require the installation of virtual, real-time anti-virus scanning software on all devices accessing the corporate network to protect from viruses and malware. This software is usually designed to detect, alert IT personnel, and contain these threats.

Although, desktop computers can easily accommodate anti-virus software, many mobile devices are constrained by memory, processing power and battery life. Thus, another approach is available to organizations to further protect their data and network by proactively preventing mobile devices from downloading or running unauthorized programs or to restrict what features and functions an application can use. For example, an organization should specify exactly which applications are permitted on the device, restrict the types of connections that a third-party application running on the device can establish (such as network connections inside the firewall), or lock all third party applications from loading onto and running on the device (BlackBerry, 2010).

## 4.3 Unified Policy Management

Studies indicate that some of the most traditional and simple security frameworks are among the most effective for businesses today, including comprehensive written BYOD policies and employee awareness training. IT departments should work with corporate executives and managers to ensure the proper lessons are being delivered to employees before the launch of BYOD or when implementing new company-wide security policies (Nielsen, 2013).

A comprehensive BYOD policy should be developed by taking into account any existing security rules to mitigate potential security risks and legal liability that naturally come with employees utilizing personal mobile devices to perform work tasks. However, at a minimum, every written industry-specific BYOD policy should address three core components to strengthen the various aspects of a BYOD program and its implementation within an organization.

### *4.3.1 Key Components to Cover*

#### 4.3.1.1 Technology, Software, and Support

There is mobile device software that exists to allow employers to enforce security policies, manage password controls, monitoring usage/ activity, manage the installation of applications and programs such as antivirus software, safeguard work-sensitive information and remotely lock/wipe devices or preserve important data when necessary. If employees will be handling sensitive information regularly, then such software tools must be considered for implementation as part of a comprehensive plan to limit security breaches (Dick & Santucci, 2013).

Once the infrastructure is ready for BYOD, the IT organization must ensure that employees can access the applications and services they need for work. Therefore, the next step is to consider how a BYOD environment will change the way IT operates. It has to determine if it needs to address a change to support models, the help desk or service-level agreements (SLAs). Particularly, the service desk now has to be prepared and trained to figure out if a reported problem is with an application that the business is trying to deliver or if it is a problem with the employee's phone. Therefore, to give the service desk a fighting chance, the IT organization should outline which devices and software versions are supported.

#### 4.3.1.2 Policies and Practices

Organizations must identify all of the devices/platforms supported by the company's network and thus permitted for use by the employees at work for work-related purposes. In addition, appropriate security protocols, such as establishing passwords or PINs, must be enforced by employers and followed by employees. To limit the potential for viruses and

malware to infect the corporate network, hacked devices will be banned and employees should be aware that companies will monitor activity/usage on devices. Employees should also be notified that business information contained on personal devices is the property of the company and that there is no expectation of employee privacy related to such information.

Policy and expectations around lost, damaged or stolen devices need to be clearly stated and communicated to the employees. It should cover the specific security actions that a company will take to protect its sensitive data if a device is lost, damaged or stolen, if data must be remotely wiped, or an employee leaves or is terminated. In addition, it should outline expectations or instructions, such as notifying the company's IT department, within a certain time period before contacting the mobile carrier if personal devices are lost, damaged or stolen. This allows IT to intervene and disable access and/or delete corporate data in a timely manner. Everyone involved in the BYOD program should know their responsibilities. Thus, employees should be required to sign updated acknowledgments and agreements that spells out their ongoing obligations under the company's BYOD plan (Dick & Santucci, 2013).

#### 4.3.1.3 Employee Education

A BYOD plan is of little use if employees are not aware of its existence or do not understand what is required of them as it relates to using personal mobile devices in the workplace. Organizations should emphasize the employee's role in protecting the data while outlining why it is important to implement security controls. Employees should receive periodic training on the company's BYOD practices and policies (Dick & Santucci, 2013). In addition, there should be a signed agreement that outlines the terms and conditions so everyone has a clear picture of the policies.

The aim is to create policies that protect corporate assets and limit liability while maximizing the user's ability to be productive, make decisions and think creatively. Once the plan has been established and corporate leaders feel comfortable with the language of BYOD policies, the next step is to implement effective enterprise mobility management solutions to help IT departments enforce the protocols (CDW'S Mobility at Work Report, 2013).

## 4.4 Aligning Mobile Strategy with the Overall Organizational Strategy

### *4.4.1 Diverse Perspectives, Collective Plan*

Mobility is no longer just a plan to develop and put in place. Mobility needs to become a complete company lifestyle that is supported and encouraged at all levels. Therefore, depending on the unique objectives and functions of an organization, ensuring that a mobility strategy that is in line with overall objectives can be difficult however the process can be simplified. Experts say it takes a team of stakeholders, representing a cross section of internal experts, to develop an overarching plan for mobility (CDW's Mobile Device Policy Report, 2013).

Therefore, it is critical for a mobility steering committee to be organized. This committee should include members from three organizational groups that will play a particularly essential role in developing a mobility strategy. These groups are information technology (IT), human resources (HR) and line-of business units. Discussing the goals, challenges and expectations around mobility can lead to new ways for these groups, particularly HR and IT, to work together. Because HR comes from a unique perspective as it is responsible for creating and distributing policies, it has to also keep in mind how to create a favorable employee experience as well. HR has the ability to balance the benefits and risks associated with mobility. The IT team can

augment this perspective by lobbying for efforts to address security and management risks, while business managers can make sure the policies address the needs of users, specifically considering how the workforce wants to and should work based on their roles and responsibilities (CDW's Mobile Device Policy Report, 2013).

These groups can help define the mobility goals as they must augment the organization's objectives and mission. In addition, it must define what challenges and opportunities the organization is trying to address with a modern mobile policy. This can range from helping the CEO, who just got a new tablet, to end users, who are pressuring the organization to support Android devices (CDW's Mobile Device Policy Report, 2013). Consideration should also include input from line-of business managers who want to put corporate data in the hands of people in the field, which represents a true business model. A final consideration is the fact that if the organization does not have a system in place to support mobility, end users will find their own way. Therefore, it must understand the drivers for this adoption and align it to meet the organization's current and future needs. These drivers may include a growing acceptance of the BYOD model, both as an opportunity for cutting IT costs and as a potential productivity booster. In addition, other incentives may include the ability to better secure an organization's data and applications, as well as making sure that workers have ready access to the necessary tools to do their jobs whether they are at work, home or on the road.

Therefore, by engaging business stakeholders and reviewing business goals and strategies, an organization can build a mobility program that aligns with its overall strategic direction. Furthermore, depending on the business, a successful BYOD program can result from

the involvement of other groups such as legal, finance and risk management. Involving all of the departments together can ensure the mobility plan:

- Promotes corporate objectives, whether this includes developing a more mobile workforce or extending an existing enterprise mobility strategy;
- Obtains executive support to avoid unrealized benefits, cost overruns and poor decision making;
- Addresses all of the necessary security issues;
- Deploys mobile technology that can be adopted and utilized in the most effective way possible;
- Provides the expected outcome with regards to productivity and security.

## 4.5 Recommendation for Real World Implementation

### *4.5.1 ETS: Organization Overview*

Educational Testing Service (ETS) is a non-profit organization that was founded in 1947. ETS advances quality and equity in education for people worldwide by creating assessments based on rigorous research. It develops, administers and scores more than 50 million tests annually, including the *TOEFL*® and *TOEIC*® tests, the *GRE*® General and Subject Tests and *The Praxis Series*™ assessments, in more than 180 countries, at more than 9,000 locations worldwide.

In addition to assessments, ETS conducts educational research, analysis and policy studies and develops a variety of customized services and products for teacher certification, English language learning and elementary, secondary and postsecondary education.

More than 3,200 employees work at ETS offices throughout the United States and the world. ETS has 10 offices in the U.S. with the headquarters located in Princeton, New Jersey. Of these, more than 2,300 of our professional staff have training and expertise in education, psychology, statistics, psychometrics, computer sciences, sociology and the humanities (ETS, 2013).

### *4.5.2 Implementing a Suitable Mobile and Security Strategy*

It is no secret that mobile devices and applications have been flooding into organizations of all types and sizes. Although ETS is neither a profit nor a technology organization, it is by no means an exception to this trend. It had begun facing similar pressures as other organizations to adopt the BYOD concepts within the workplace. Consequently, six months ago, ETS had implemented a BYOD program. It has since realized a substantial increase in employee interest and requests for BYOD enrollment. Therefore, a mobility steering committee that includes key members from IT, HR, business units and legal along with business managers, has been organized. The committee has been tasked with devising and implementing an enterprise mobility strategy that is aligned with the overall business objectives.

The development of the enterprise mobility strategy should follow these steps to ensure all required aspects are considered before implementation:

- Define success for BYOD in your organization;
- Define and document BYOD user policies;
- Apply end-point and network security measures to ensure that it can accommodate an influx of BYOD user devices;

- Implement security infrastructure via Enterprise Mobility Management (EMM), mobile VDI, virtualization, or a hybrid solution that meets organization's requirements;
- Define collaboration and document-level security for BYOD devices;
- Provide end-user training in your program policies and security; require signed agreement from employees (Kelly, 2013).

As part of the strategy, IT had conducted a thorough review of the existing wireless infrastructure and the security settings to determine if the network can handle the increasing number of devices and whether or not corporate data remains secured. The review had revealed these concerns and recommendations based on the mobility strategy options:

Network

- Concern: The "hub and spoke" architecture for ETS has reached its end-of-life due to the increase in mobile devices and applications being utilized. The wireless network is overly congested due to growth and use of mobile devices integrated with the 802.11n technology. The technology has greatly increased traffic on the network due to the multitude of devices that are equipped with this technology. The traditional architecture was not originally designed to handle the high amount of traffic.
- Recommendation: A recommended solution is to upgrade the traditional wireless infrastructure to a distributed intelligence infrastructure, where the network will provide adequate wireless and reliability within the organization. The new infrastructure will provide built-in redundancies and continual service, due to the nature of distributed network technology. It is designed to enhance network performance and traffic without sacrificing QoS of applications and mobility. The traditional architecture was centralized and that helped

with costs with older 802.11b/g solutions. With increased network traffic, it created a choke point at the centralized controller, thus impacting the network. To meet these needs, a distributed intelligence architecture can provide the full benefits of what 802.11n technology has to offer.

- Concern: The access and performance was degraded due heavy network load of connected mobile devices and application use.

- Recommendation: To resolve this concern, it is recommended to have an optimization solution for the wireless network. User optimization was presented to provide quick and secure access for mobile devices on the network. It is necessary to select a proper access manager solution that allows employee devices to be quickly and seamlessly authenticated and identified on the network once given access. Application optimizations help enable effective controls to ensure expected performance. Utilizing application control technology will help mitigate any degradation in business-critical application use on the network. This solution will help optimize any wireless performance deficiencies.

Policy

- Concern: There is no written company policy requiring employees to lock their personal devices used for work purposes with minimal authentication, which is password protection. This opens up potential risk for confidential data to be accessed by unauthorized users if a device is lost or stolen.
- Recommendation: Because the key to protecting stored information is preventing access at the device level, the company policy should clearly state and require all mobile devices to be password protected. In cases where heightened security is needed, the use of smart cards,

biometrics or other similar mechanisms are options that can easily provide stronger protection against unwanted access to mobile devices.

Security measure for lost/stolen devices

- Concern: ETS currently does not have a security measure in place to address the consequences of a lost or stolen personal device that was used to access corporate applications/data. This is a major concern as it can lead to an unauthorized user obtaining access to the device, especially if the device was not minimally password-protected, which can further lead to the potential loss of confidential data.
- Recommendation: ETS should consider utilizing the remote lock/ wipe capability that can allow IT to remotely disable access and delete corporate data on the mobile device. Although there are liability issues with regards to employers potentially deleting personal data along with company data, the users should be made aware of the policy and be required to sign and acknowledge with written consent. In addition, the policy should state the users must report lost or stolen devices within a certain time period, so IT can intervene to take action to mitigate data loss. Because this feature is already available in the MDM solution, a separate security measure to address this security issue is not required.

Enterprise management and security

- Concern: Lack of a unified management and security capability to handle the issues around device management, application management, and security of the corporate data should be segregated from the personal data on the mobile devices.

- Recommendation: ETS should consider implementing the EMM suite that includes the MDM and MAM solution. MDM is a single management panel to easily secure and enable access to resources at an aggregate, departmental, user group, or device level. It will allow administrators to enroll and manage assets on the network, configure settings, remotely locate and wipe devices, distribute software, track usage and enforce corporate policies relating to passwords and other security measures, across all operating systems including Macs/iOS, Android, and BlackBerry.
- Although ETS is already quite familiar with the Desktop VDI technology, mobile VDI will not be recommended as an enterprise management and security solution at this time due to its major constraints. These constraints include a high probability that some applications running on the mobile VDI will not display well or be unable to function at all on a smartphone or tablet with these factors:
    - over any VDI interface;
    - be greatly slower on some older, underpowered devices;
    - be greatly slower over slow links;
    - without a keyboard, or;
    - without a traditional input device (mouse, track pad or pointer).

Based on research and expert advice, it has been recommended for ETS to migrate to their enterprise mobile strategy with the necessary network and management system upgrades in a controlled fashion. Therefore, it would be ideal to migrate in stages so that it is manageable, enhances productivity and maintains security for all users involved. In addition to significant planning and considerations that need to take place, this approach will become more workable

for teams who are well-adapted to older methods and will have a harder time shifting to complete mobility without a gradual progression. Ultimately, this plan will allow ETS to embrace device proliferation by creating a mobile environment that provides end users the information they need and experiences they desire no matter the time, place or device.

Because technology is constantly changing, ETS should examine and reexamine whether or not its strategy is working and what else needs to be done to keep growing and improving. This can mean revisiting the market every six to 12 months to evaluate if something better is available. The technology is evolving rapidly and the solutions market will converge quickly, therefore there is no need to over-invest in a fixed solution and assume you are done (Baker, 2012).

# 5 Conclusion

Mobile devices have become more persistent in businesses today than in previous generations of computing. Mobile applications on these devices are used for both personal and business purposes. Because mobility is one of the key drivers of technology today, organizations are embracing the concept of IT consumerization/ BYOD into the workplace. From increased employee satisfaction and productivity to lower IT equipment and operational expenditures, companies have recognized that mobile devices are reasonably essential to their own success. However, many organizations are facing significant challenges with the explosion of mobile devices being used today along with provisioning the appropriate supporting infrastructure due to the unprecedented demands on the wireless and network infrastructures. The security risks posed

by the implementation of mobile technology are also significant. Careful planning and review is needed to make sure all loopholes are identified and secured. Managing mobility along with securing corporate assets have become difficult tasks for IT professionals as many organizations underestimate the potential security and privacy risks of using wireless devices to access organizational resources and data.

Therefore, in order for organizations to prepare to address the needs and requirements of a new mobile workforce, they must implement a suitable mobile strategy by:

- Organizing a mobility steering committee;
- Identifying the latest challenges presented;
- Assessing the current IT infrastructure and security environment;
- Developing an enterprise mobility strategy;
- Aligning with the organizational goals;
- Informing and educating employees;
- Implementing a phased approach;
- Continually examining the strategy to keep growing and improving.

Because technology is constantly changing, organizations should examine and reexamine whether or not their strategy is working and what else needs to be done to keep growing and improving. In addition, there is not one specific solution or strategy when it comes to every individual company; therefore, it is very important to really focus on the organization's specific security strategy and mobility objectives. Understanding what is truly needed to offer the best mobile security for the organization will help the IT professional make the ideal decision. Therefore, with the approaches outlined in this analysis, organizations must keep in mind that mobility is more about enabling mobile workers by giving them the tools they need to do their

jobs better rather than implementing the latest technologies available that may not be suitable for the organization's overall strategic direction.

# 6 Lessons Learned

We have learned from our research that there isn't one solution or strategy that can be applied to every individual company. There is no one size fit all recommendation that can resolve all of the challenges we discussed. It is important for companies to focus on their specific security challenges and mobility objectives to find the right solution.

In addition, many of the solutions we had recommended have been around for a few years and although they meet certain standards to address issues, they are still flawed in some ways because technology and the challenges are constantly changing.

# 7 Considerations for Future Research

In regards to future research, we recommend the following:

## 7.1 Mobile Printing

Mobile devices were not designed for printing, nor were printers designed to talk to anything other than a PC or a Mac (Null, 2013). The device and the printers may need to be on the same wireless network, or the printer may need access to the Internet. Some applications can send the print job via email to the printer, in which case, the user could be anywhere when he or she sends the job. While the applications offer some ability to customize the job—such as

number of prints, or size or type of paper—the printouts might not look exactly like what the user expects, because the applications cannot translate all of the fonts or formatting perfectly (Null, 2013). Organizations should research and evaluate enterprise-wide solutions that include some form of mobile printing capabilities for their mobile workforce.

## 7.2 Cost differences of solutions

Organizations should evaluate the cost of various solutions that are available along with the hardware and software that is required to support them.

## 7.3 Advancement in Cloud services

The cloud technology is still very new and therefore there is a lot that needs to be considered when it comes to mobile security and access management for corporate data on the cloud. Organizations should continue to research this technology and determine its usability along with security implications for storing confidential data.

# 8 Appendix A – List of Acronyms

| | |
|---|---|
| 3DES | Triple Data Encryption Standard |
| 3G | Third Generation |
| 4G | Fourth Generation |
| AES | Advanced Encryption Standard |
| AP | Access Point |
| BYOD | Bring Your Own Device |
| CALEA | Communication Assistance for Law Enforcement Act |
| CEO | Chief Executive Officer |
| CPU | Central Processing Unit |
| CTO | Chief Technology Officer |
| DLP | Data Loss Prevention |
| DMZ | Demilitarized Zone |
| DPI | Deep Packet Inspection |
| EMM | Enterprise Mobility Management |
| ETS | Educational Testing Service |
| GB | Gigabyte |
| GPU | Graphics Processing Unit |
| GRE | Graduate Record Examinations |
| HD | High-Definition |
| HIPAA | Health Insurance Portability and Accountability Act |
| HR | Human Resources |
| HTML | HyperText Markup Language |

| | |
|---|---|
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IDC | International Data Corporation |
| IEEE | Institute of Electrical and Electronics Engineer |
| IT | Information Technology |
| Kbps | Kilobits per second |
| LAN | Local Area Network |
| MAM | Mobile Application Management |
| MB | Megabyte |
| Mbps | Megabits per second |
| MDM | Mobile Device Management |
| NAC | Network Access Control |
| NMS | Network Management System |
| OS | Operating System |
| PC | Personal Computer |
| PIN | Personal Identification Number |
| QoS | Quality of Service |
| RF | Radio Frequency |
| SD | Secure Digital |
| SLA | Service-Level Agreement |
| SNR | Signal-to-Noise Ratio |
| SOX | Sarbanes–Oxley |
| SSL | Secure Socket Layer |
| TCO | Total Cost of Ownership |
| TLS | Transport Layer Security |

| | |
|---|---|
| TOEFL | Testing of English as a Foreign Language |
| TOEIC | Testing of English for International Communication |
| USB | Universal Serial Bus |
| VDI | Virtual Desktop Infrastructure |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |
| WMN | Wireless Mesh Networks |

# 9 Bibliography


1. Accudata systems (2013). Retrieved from http://www.accudatasystems.com/assets/byod-360-degree-planning.pdf
2. Adamson, M. (2012, July 11). *MDM, MAM, EMM: It's all About What's Important to Your Organization | Mobile Device Management News, BYOD Best Practices and Buyers Guide, MDM Software*. Retrieved from http://solutions-review.com/mobile-device-management/mdm-mam-emm-whats-important-organization/
3. Aerohive (2012). *High-Density Wi-Fi Design Principles*. Retrieved from http://www.aerohive.com/pdfs/Aerohive-Whitepaper-Hi-Density%20Principles.pdf
4. Anderson, N. (2013). *Cisco Bring Your Own Device Device Freedom Without Compromising the IT Network*. Retrieved from http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf
5. Athow, D. (2013, September 14). *"Enterprises are being ignorant towards the issues BYOD can and are causing to their business" says Acronis | ITProPortal.com*. Retrieved from http://www.itproportal.com/2013/09/14/enterprises-are-being-ignorant-towards-the-issues-byod-can-and-are-causing-to-their-business-says-acronis/#ixzz2mjkBZOa9
6. Baker, P. (2012, April 11). *BYOD management tools and tactics*. Retrieved from http://www.cioupdate.com/technology-trends/byod-management-tools-and-tactics.html
7. BlackBerry (2010). *The CIO's Guide to Mobile Security*. Retrieved from http://us.blackberry.com/content/dam/blackBerry/pdf/cioGuide/RIM_CIO_GuidetoMobileSecurity.pdf

8. Bokhari, F., & Zaruba, G. (2012). *ON THE USE OF SMART ANTS FOR EFFICIENT ROUTING IN WIRELESS MESH NETWORKS* (2). Retrieved from http://arxiv.org/ftp/arxiv/papers/1209/1209.0550.pdf
9. Bort, J. (2012, October 5). *Managing An Explosion Of Mobile Devices And Apps In The EnterpriseEmbargo Zone | Embargo Zone*. Retrieved November 11, 2013, from http://www.embargozone.com/2012/11/05/managing-an-explosion-of-mobile-devices-and-apps-in-the-enterprise/
10. CDW's Explosion of BYOD (n.d.). *The Explosion of BYOD*. Retrieved from http://webobjects.cdw.com/webobjects/media/pdf/Solutions/mobility/CaseStudy-Johnson-County.pdf
11. CDW's Mobile Device Policy Report (2013). *8 Steps to an effective Mobile Device Policy*. Retrieved from CDW website: http://webobjects.cdw.com/webobjects/media/pdf/Solutions/Mobility/Mobile-Device-Policy.pdf
12. CDW'S MOBILITY AT WORK REPORT (2013, September 9). *MOBILITY AT WORK: MAKING PERSONAL DEVICES A PROFESSIONAL ASSET*. Retrieved from http://webobjects.cdw.com/webobjects/media/pdf/Solutions/Mobility/CDW-Mobility-at-Work-Report-090613.pdf
13. CDW's Take Security to Go Report (2012). *Take Security To Go*. Retrieved from http://webobjects.cdw.com/webobjects/media/pdf/Solutions/Security/121700-Take-Security-To-Go-Mobile-Security-BYOD.pdf
14. CDW's TMM Solutions (2013). *Total Mobility Management Solutions by CDW*. Retrieved October 25, 2013, from http://www.cdw.com/content/solutions/mobility/mdm-mobile-device-management.asp
15. Cisco (2007). *Antenna Patterns and Their Meaning [Cisco Aironet Antennas and Accessories] - Cisco Systems*. Retrieved from

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.html

16. Cisco (2013). *Cisco Bring Your Own Device [Design Zone for Enterprise Networks] - Cisco Systems*. Retrieved from http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.html
17. Cisco (2013, February 6). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012? 2017 - Cisco Systems*. Retrieved from http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html
18. Cisco (2007, July 11). *Network Management System: Best Practices White Paper - Cisco Systems*. Retrieved from http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml
19. Dell (n.d.). *Is Your Infrastructure? Mobile Ready??* Retrieved from http://i.dell.com/sites/content/business/smb/sb360/en/Documents/wp-mobile-connectivity.pdf
20. Deloitte (n.d.). *Bring your own device Unlock value for your organization*. Retrieved from http://www.deloitte.com/assets/Dcom-Norway/Local%20Assets/Documents/Publikasjoner%202012/Deloitte_bring_your_own_device_092112.pdf
21. Detwiler, B. (2013, February 6). *The Executive's Guide to BYOD and the Consumerization of IT (free ebook) | ZDNet*. Retrieved from http://www.zdnet.com/the-executives-guide-to-byod-and-the-consumerization-of-it-free-ebook-7000010871/
22. Defining the future of wireless networking architecture. (2011). *Communications Today,* Retrieved

from http://search.proquest.com/docview/898472024?accountid=11999

23. Developing Solutions (n.d.). *Use Case: Testing DPI within an Existing PDN | Developing Solutions, Inc*. Retrieved from http://www.developingsolutions.com/solutions/use-case-testing-dpi-within-an-existing-pdn/
24. Dick, T., & Santucci, A. (2013, July 16). *Security Is Key To "BYOD" Policies*. Retrieved from http://www.jdsupra.com/legalnews/security-is-key-to-byod-policies-98689/
25. Dondurmacioglu, O. (2013, April 22). *Top-5 Bandwidth Hungry Mobile Apps on a Wireless LAN | Aruba Networks*. Retrieved from http://www.arubanetworks.com/blogs/top-5-bandwidth-hungry-mobile-apps-on-a-wireless-lan/
26. EMA (2013, January). *Seven Best Practices for Network Management (Analyst report/4AA4-5440ENW.pdf)*. Retrieved from http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-5440ENW
27. ETS (2013). *About ETS*. Retrieved from http://www.ets.org/about
28. Forbes (2013, November 6). *XeroxVoice: Five Ways to Reduce BYOD Security Risks - Forbes*. Retrieved from http://www.forbes.com/sites/xerox/2013/11/06/five-ways-to-reduce-byod-security-risks/
29. Furbush, J. (2012, February 24). *BYOD strains corporate wireless network bandwidth*. Retrieved from http://searchconsumerization.techtarget.com/news/2240118466/BYOD-strains-corporate-wireless-network-bandwidth
30. Gilby, C. (2008). Mobile devices impact WLANs. *Communications News, 45*(1), 28-29.
31. Gittlen, S. (2012, January 4). *Bandwidth bottlenecks loom large in the cloud - Computerworld*. Retrieved from http://www.computerworld.com/s/article/9223117/Bandwidth_bottlenecks_loom_large_in_the_cloud

32. Goldberg, T. (2013). *Securing Your Enterprise Data in a BYOD World*. Retrieved from http://www.ittoday.info/Articles/BYOD_World.htm

33. Hetrick, V. (2012, August 14). *Study: Organizations lack BYOD policies, employees lack awareness | www.maas360.com*. Retrieved from http://www.maas360.com/news/industry-news/2012/08/study-organizations-lack-byod-policies-employees-lack-awareness/

34. Hill, K. (2013, September 10). *Survey: BYOD posing major challenges for networks, management | Mobile Technology | Wireless Broadband | Wireless Carriers | RCR U.S. Wireless NewsMobile Technology | Wireless Broadband | Wireless Carriers | RCR U.S. Wireless News*. Retrieved from http://www.rcrwireless.com/article/20130910/enterprise_mobile_and_wireless/survey-byod-posing-major-challenges-for-networks-management/

35. Janssen, C. (n.d.). *What is a Network Management System (NMS)? - Definition from Techopedia*. Retrieved from http://www.techopedia.com/definition/11988/network-management-system-nms

36. Johnson, K. (2012). *SANS Mobility/BYOD Security Survey*. Retrieved from http://www.sans.org/reading-room/analysts-program/mobility-sec-survey

37. Kelly, W. (2013, November 27). *Define BYOD for your organization.* Retrieved from http://www.techrepublic.com/blog/smartphones/define-byod-for-your-organization/

38. Kerravala, Z. (2012, September). *Bring-Your-Own-Device Requires New Network Strategies*. Retrieved from http://www.xirrus.com/cdn/pdf/zeusk_byod_requires_new_network_strategies

39. Kozup, C. (2013, January 14). *Guest blog: Apps in the workplace? Yes we can - Computer Business Review*. Retrieved from http://www.cbronline.com/blogs/cbr-rolling-blog/guest-blog-apps-in-the-workplace-yes-we-can-140113

40. Lancos, K. (2012, March 30). *Mobile Data Growth and What it Means for You | Visual.ly*. Retrieved from http://visual.ly/mobile-data-growth-and-what-it-means-you

41. Manire, R. (2012, August 8). *Rethinking Mobile Infrastructure: The New Last Mile « Breaking Government - Government news, analysis and commentary*. Retrieved from http://breakinggov.com/2012/08/08/rethinking-mobile-infrastructure-the-new-last-mile/

42. Marko, K. (2011, July 27). *Keeping Corporate Data Off Mobile Devices With VDI*. Retrieved from http://www.informationweek.com/mobile/keeping-corporate-data-off-mobile-devices-with-vdi/d/d-id/1099220

43. Mathias, C. (2012, September 17). *Enterprise mobility management options: MDM, MAM and MIM*. Retrieved from http://searchconsumerization.techtarget.com/tip/Enterprise-mobility-management-options-MDM-MAM-and-MIM

44. McLellan, C. (2013, February 1). *Consumerization, BYOD and MDM: What you need to know*. Retrieved October 28, 2013, from http://www.zdnet.com/consumerization-byod-and-mdm-what-you-need-to-know_p3-7000010205/

45. Mehra, R. (2011). *Bring Your Own Device (BYOD): What is the Impact on the Enterprise Network*. Retrieved from http://www.sysbus.eu/wp-content/uploads/2012/02/BYOD.pdf

46. Mehra, R. (2013, February). *Enabling Organizational Agility with New Campus Network Architectures*. Retrieved from http://www.brocade.com/downloads/documents/white_papers/idc-enabling-organizational-agility-wp.pdf

47. Messmer, E. (2013, March 28). *Forrester Research calls mobile-device management 'heavy-handed approach' - Network World*. Retrieved from http://www.networkworld.com/news/2013/032813-forrester-mobile-268206.html?page=2

48. Mitchell, B. (n.d.). *802.11n Wi-Fi in Computer Networking*. Retrieved December 2, 2013, from http://compnetworking.about.com/od/wireless80211/g/bldef_80211n.htm

49. Mobile VDI (2013). *Virtual Desktop Infrastructure Goes Mobile*. Retrieved from

http://webobjects.cdw.com/webobjects/media/pdf/Solutions/Mobility/Mobile-Virtual-Desktop-White-Paper.pdf

50. Motorola (2011, April). *DistributeD intelligence: The Future of Wireless netWorking Architecture*. Retrieved from http://www.motorolasolutions.com/web/Business/Solutions/Network_Technologies/WiNG-5_WLAN/_Documents/_Staticfiles/WiNG5_WhitePaper_DistributedIntelligence.pdf
51. Nagy, A. (2012). *High-Density Wi-Fi Design Configuration Guide*. Retrieved from http://www.aerohive.com/330000/docs/help/english/5.1r2/ref/Aerohive_High-Density_Wi-Fi-Design-Config-Guide_330073-01.pdf
52. Nielsen, J. (2013, October 22). *Security policy musts for BYOD*. Retrieved from http://www.maas360.com/news/industry-news/2013/10/security-policy-musts-for-byod-523768/
53. Null, C. (2013, September 16). *Mobile printing: A guide for the BYOD world | PCWorld*. Retrieved from http://www.pcworld.com/article/2048634/mobile-printing-a-guide-for-the-byod-world.html
54. Ouellette, N., & Thomas, D. (2011). Network access control (NAC). *SC Magazine, 22*(9), 36. Retrieved from http://search.proquest.com/docview/895047169?accountid=11999
55. P2pfoundation (n.d.). *Mesh Networks - P2P Foundation*. Retrieved from http://p2pfoundation.net/Mesh_Networks
56. Panzarino, M. (2012, February 13). *1B Mobile Users by 2016, Apple, Google and Microsoft with 90% share*. Retrieved from http://thenextweb.com/mobile/2012/02/13/forrester-1b-smartphone-users-by-2016-with-apple-google-and-microsoft-powering-90/
57. Phifer, L. (2012, December 7). *MDM plus MAM tools equals a one-two punch for BYOD admins*. Retrieved from http://searchconsumerization.techtarget.com/tip/MDM-plus-MAM-tools-equals-a-one-

two-punch-for-BYOD-admins

58. Phifer, L. (2013, March 4). *Mobile device management checklist*. Retrieved from http://searchconsumerization.techtarget.com/tip/Mobile-device-management-checklist
59. Phneah, E. (2013, February 4). *Five security risks of moving data in BYOD era | ZDNet*. Retrieved from http://www.zdnet.com/five-security-risks-of-moving-data-in-byod-era-7000010665/
60. PWC (2011, November). *The consumerization of IT The next-generation CIO*. Retrieved from http://www.pwc.com/en_US/us/technology-innovation-center/assets/consumerization-information-technology-transforming-cio-role.pdf
61. Rubens, P. (2013, February 21). *Cloud Wi-Fi Could Become Key for Network Management*. Retrieved from http://www.enterprisenetworkingplanet.com/netsysm/cloud-wi-fi-key-for-network-management.html
62. Ruckus Wireless (n.d.). *Ruckus Wireless*. Retrieved from http://www.ruckuswireless.com/
63. Scarfone, K. (2013, November 20). *How to Help DLP and Encryption Coexist*. Retrieved from http://www.edtechmagazine.com/higher/article/2013/11/how-help-dlp-and-encryption-coexist
64. Sophos (2013, July 13). *Sophos Mobile Device Management Buyers Guide*. Retrieved from http://i.zdnet.com/whitepapers/Sophos_Mobile_Device_Mgmt_Buyers_Guide_July13.pdf
65. Solarwinds (n.d.). *What is Network Device Management*. Retrieved from http://www.solarwinds.com/it-management-glossary/what-is-network-device-management.aspx
66. Spain, C. (2013, October 21). Mobile Devices Will Transform Your Business IT [Web log post]. Retrieved from http://blogs.cisco.com/wireless/mobile-devices-will-transform-your-business-it/
67. Strong, A. (2012, August 31). *Enlisting the help of infrastructure to cope with the BYOD explosion*. Retrieved from http://www.networkworld.com/news/tech/2012/083112-infrastructure-byod-262085.html

68. VMware (2013, April). *The BYOD Opportunity*. Retrieved from http://www.vmware.com/files/campaigns/englishhtml/VMware-BYOD-Opportunity-Whitepaper.pdf

69. Weber, M. (2013, September 18). *Coalfire - IT GRC Compliance and Security Blog from Coalfire*. Retrieved from http://www.coalfire.com/The-Coalfire-Blog/September-2013/BYOD-Survey-2013-Employees-and-Companies-Remain-La

70. Webopedia (n.d.). *What is AP? - A Word Definition From the Webopedia Computer Dictionary*. Retrieved December 1, 2013, from http://www.webopedia.com/TERM/A/AP.html

71. Xirrus (2013). *Optimize Your Wi-Fi Network*. Retrieved from http://www.xirrus.com/cdn/pdf/xirrus_optimize-wi-fi-network-wp_v4_031913

72. Yahoo (2013, June 25). *BlackBerry Secures iOS and Android in the Enterprise Without Sacrificing the User Experience - Yahoo Finance*. Retrieved from http://finance.yahoo.com/news/blackberry-secures-ios-android-enterprise-120000355.html