BYOD: The Next Wave of Consumerization of IT
The Impact of BYOD on the Enterprise IT Landscape

Ivan I. Ivanov
Empire State College of the State University of New York,
Long Island Center, Hauppauge, NY, U.S.A.
ivan.ivanov@esc.edu

Keywords: Bring Your Own Device – BYOD, Consumerization of IT, Company-Owned, Personally-Enabled – COPE, Mobile Device Management – MDM, Mobile Application Management – MAM, Mobile Content Management – MCM, BYOD Framework

Abstract: In the last few years, new technologies emerge first in the consumer market and then, after mass acceptance, are employed largely by business organizations. Companies across the globe are going through the most disruptive new technology development: Consumerization. Consumerization of IT, along with workforce mobility, and flexible, reliable, accessible and affordable remote computing, are forcefully changing the corporate IT lanscape, affecting the relationship between enterprise IT, knowledge workers, corporate users, and consumers. This phenomenon advances with every arrival of new devices, applications, or strategic trends such as Bring-Your-Own-Device (BYOD). BYOD is currently a growing trend in the private and public sector that allows employees the convenience of logging into the corporate network with their personal mobile devices. This paper explores the impact of this trend on the enterprise IT landscape and provides a decision framework for BYOD adoption.

1 CONSUMERIZATION OF IT – THE AGE OF THE CUSTOMER

Current trends in IT utilization show that new technologies emerge first in the consumer market and then, after mass acceptance, are employed largely by business organizations. The expected consequence of this pattern is that across the globe companies are experiencing the most disruptive new technology trend of this decade: Consumerization.

The process of Consumerization is well depicted by Forrester Research report from June 6, 2011, "Competitive Strategy in The Age Of The Customer." This is the phenomenon of employees using devices, applications, and web services to actually empower business users or employees to innovate (Forrester Consulting, 2013).

Consumerization of the IT is actually advancing swiftly with every arrival of new devices, strategic trend, or applications. The oportunities for business users, ranging from consultants, hightech professionals and executives, to administrative assistants, and sales and call center representatives, to leverage consumerized offerings – those offered outside of organizational IT – varies depending on the business policy and openness.

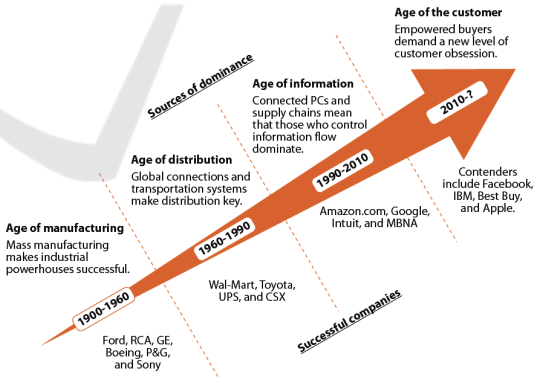

Figure 1: Consumerization of IT. Adopted from "Competitive Strategy in The Age Of The Customer," Forrester Research, Inc. June 6, 2011.

Consumerization of IT, along with workforce mobility, and flexible, reliable, accessible and affordable remote computing, are forcefully changing the corporate IT lanscape affecting the relationship between enterprise IT, knowledge workers, corporate users, and consumers. For company IT management, consumerization

Ivanov I.
BYOD: The Next Wave of Consumerization of IT The Impact of BYOD on the Enterprise IT Landscape.
DOI: 10.5220/0005426702450251
In *Proceedings of the Fourth International Symposium on Business Modeling and Software Design (BMSD 2014)*, pages 245-251
ISBN: 978-989-758-032-1

exemplifies the convergence of a demanding set of challenges such as information and infrastructure security, technology policy, data protection, and end-user technology. For corporate management, consumerization of IT signifies a new strategy which supports business models and process innovations, talent strategy and customers' satisfaction, as well as corporate brand and identity.

Consumerization of IT blurs the line between personal and work life, especially for mobile workers. Mobile workers make up about 39% of the employees in Noth America, 25% in Europe, and 42% in Asia, with a growing tendency according to Forrester's analysis (Forrester Consulting, 2013). Their cohort benefits the business immensely by increasing productivity, and advancing collaboration and business agility, thereby improving customer satisfaction and climbing the rate of talent retention. Consumerized employees spread the boundaries of the workday and workplace, and it is fair to name them "anytime, anywhere workers."

2 BYOD – OPPORTUNITIES, CHALLENGES, GAINS

BYOD, or Bring-Your-Own-Device, is a growing trend in the private and public sector that allows employees the convenience of logging into the corporate network with their own personal devices. The rise of the mobile workforce to 1.2 billion in 2013, representing 35% of the worldwide workforce according to IDC Forecast, drives strongly the BYOD initiative as many of those workers will be using their own devices (International Data Corporation IDC, 2012).

The BYOD trend, as it is driven mostly by current Consumerization of IT in the enterprise, is forcing companies to redesign or create new policy and rules on how smart portable devices can be used for both corporate and private purposes, and how the related expenditures should be covered.

2.1 BYOD as Mobile Workforce Advancement

BYOD can be facilitated through applications that are native to the device, downloaded or installable applications, or even a mobile web browser. The BYOD boom originated via two converging trends: the need for employees to be responsive in a global, always-connected world, and the desire to save money by not replicating a device that employees may already own.

BYOD eliminates time boundaries, allowing employees to be productive during and after working hours. It offers flexibility, allowing them the ability to be connected to the corporate network and do some work, for example, during a child's baseball game in the afternoon as well as later in the evening. While BYOD offers flexibility and efficiencies, the initiative also brings a significant advantage to overall productivity through timely reactions and collaborative interactions. Mobility obviously brings significant improvement and added opportunities to the business environment, but as with many advantages, there are consecutive tradeoffs.

2.2 BYOD – Challenges and Concerns

A considerable challenge for an IT department is how it can effectively secure and manage the corporate network and information systems access for user-owned devices. For example, these devices cannot easily be identified, and therefore cannot be managed by the traditional IT department security settings. When employees bring in their own devices, IT loses significant control as it does not know where the device has been or what applications the user has downloaded, or what device has been introduced into the network.

Apart from legal and ethical issues, some of the noteworthy technical concerns of a BYOD program are as follows:

- delivering secure, remote access for mobile devices, while continuing to enforce granular access controls on network resources,
- securing corporate and personal data and mobile devices from malware, viruses and malicious applications, and
- mitigating the risk of loss, theft or exploitation of corporate and personal data residing on mobile devices.

From an ethical and legal standpoint, BYOD issues include corporate guidelines of what is considered "acceptable use" for actions an employee can take on their own device. Several laws have already been released regarding BYOD which include having employees sign an acceptable use agreement stating that the device can be seized for an indeterminate amount of time if the data on it is part of a legal dispute. Employees may have a real issue with their employers dictating to them what they can and cannot do on their own personal devices. It is imperative that businesses, schools, and

other organizations establish a system of accountability if they allow a BYOD policy.

Privacy concerns are at the top of the list when it comes to legal issues regarding BYOD initiatives. Convergence of both personal and corporate data and applications presents a complex issue. Will the employer be permitted to access an employee's own e-mails and text messages on a personal smartphone or tablet used by that employee at work? Other considerations include access to browser history and installed software. This is a multifaceted problem that companies have to strategize prior to the adoption of a BYOD policy. Along with an acceptable use policy, many companies also educate employees as to what constitutes acceptable use. Adherence to the policy is only effective if there has been proper education for employees and whoever else has access to corporate information.

Some companies, such as IBM, instituted policies that banned its 400,000 employees from using two popular consumer applications over concerns about data security. The company banned cloud storage service Dropbox, as well as Apple's personal assistant for the iPhone, Siri. Siri listens to spoken requests and sends the queries to Apple's servers where they are deciphered into text. Siri can also create text messages and emails on voice command, but some of these messages could contain sensitive, proprietary information.

2.3 The Business Sense of BYOD

While BYOD offers flexibility and efficiencies, the initiative brings a significant advantage to productivity. The quarterly Mobile Workforce Report from iPass Company found that many employees are working up to 20 additional hours unpaid as a result of the companies' BYOD policy (ComputerworldUK, 2012).

The 2013 iPass/MobileIron Mobile Enterprise Report depicts the tendency of increasing usage of employee-owned smart devices from 42% in 2011 to 47% in 2012, while the percentage of smartphones provisioned by employers declined from 58% to 49% for the same period (Appcelerator, Inc., 2013). Executives actually stimulate the process of establishing corporate guidelines and policies to foster BYOD adoption. According to the same report, 56% of the IT managers in 2012 confirmed that their IT policies had become more responsive and flexible to employees' demands of utilizing personal devices for dual corporate and private usage.

3 BYOD – STRATEGY AND GOVERNANCE

At this time, for many organizations, BYOD has remained an informal practice and an escalating IT complexity because of this mess-up exposes those institutions to risks from security and compliance gaps. BYOD policy can vary substantially for different organizations depending on their priorities, industry regulations, or operational models. A successful BYOD program would combine effective infrastructure and data security with easy personal use.

3.1 BYOD and Mobile Management Solutions

The IT department should provide users with secure access to corporate applications and data, while adding role-based access control and security settings of personally-owned devices to prevent the organization against data loss and non-compliant usage. The lack of standartization reflects the diversity of devices and operating systems that IT departments must grapple with days, and actually creates market opportunity for mobile management providers (iPass Inc., 2013).

3.1.1 Mobile Device Management

An important component in deploying a BYOD program is the ability to manage the mobile devices that would interface with the enterprise network. Mobile device management (MDM) is the software solution that allows a network administrator to manage and control mobile devices such as smartphones and tablets. Ideally, the MDM should be able to interface with all types of mobile devices, operating systems, and the apps they run. Another consideration is the MDM must be able to operate with a number of providers used by employees. Typically in a corporate landscape, business-owned devices will use only one wireless service provider, but in a BYOD environment, employee-owned devices each have their own wireless providers and as a result, the MDM system will have to work with dozens of service providers.

The main purpose of an MDM system is to optimize the functionality and capabilities of the workforce mobile device while keeping the business IT infrastructure and data secure. Network administration in an MDM includes the ability to interface with the enterprise's current servers and systems so that it can manage and secure corporate-

owned data and applications; synchronize with the mobile devices for file sharing, sending out patches, and add and remove devices from the network, and all these tasks must be able to be done directly over carrier networks.

By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM should be able to prevent network and system exposure from a variety of threats. One of the leading mobile device management solutions is the MobileIron MDM system. This MDM software is part of the MobileIron IT Platform which provides a "turnkey" ability to have the mobile device user to interface with the corporate backend just by downloading an app. Once the device is authenticated and activated in the network, the user has access to all resources and content they have permission to access. Like with IT networks, mobile device management is one layer of a secure BYOD program. Device management is just the beginning and is the foundation to mobile application management (MAM) and mobile content management (MCM) implementation – the two other services needed to support BYOD initiatives.

3.1.2 Mobile Application Management

As MDM focuses on the management of mobile devices, mobile application management (MAM) focuses on the management of the applications used by mobile workers. This tool allows system managers to monitor, provision, install and uninstall, update, and audit software programs and applications for mobile devices. MAM functions similarly to network system management tools used within a network environment, but it is designed specifically to work with the unique characteristics of a mobile device. Management of a variety mobile devices in a BYOD requires the ability to manage different operating systems and integrate with the wireless service providers used by the employee. Another issue unique to mobile devices application management is that apps typically are installed using the pull method initiated by the user and not the push method. Additionally, some apps require payment before installation.

MAM addresses these two issues by allowing managers to create a catalog or app storefront of internally developed business apps, as well as making available license files or tokens for approved public apps so there is no need for users to pre-pay prior to installation. For example, Mobile Application Distribution Library is a customizable app distribution tool offered by MobileIron. The library makes public and private apps available to its end users to install on their mobile devices. In addition, internally developed apps can be made available to users without having to publish them in a storefront such as Apple App Store or Android Market (MobileIron, 2014).

Security is another function of the MAM. Mobile workers will access sensitive data and the backend systems using a variety of apps. It is imperative that the apps comply with organization policies and are properly validated and encrypted. As mobile device computing grows, the number of apps has increased and malicious apps have become as ubiquitous as the safe apps. The highest priority for MAM is to protect data that moves throughout mobile workflows as well as protect its backend system from these types of apps. Some of the approaches of MAM are to allow managers to configure application settings, profiles and credentials for enterprise authentication. MAMs also monitor application usage by observing traffic and application connections. These observations may generate reports and logs that can identify issues within the network and mobile device connections.

Mobile App Containerization is one of the most advanced MAM solutions offered by Good Technology that actually does not require a mobile device management system. Containerization protects data transfer through the use of strong separation of personal and business apps and data. Containerized apps ensure that the enterprise security protocols and encryption throughout the transmission remain constant and consistent until the employees have completed their task. In addition, this method allows the manager to wipe company-owned data and apps only from a lost or stolen device; personal data is not touched at all. This actually addresses a major BYOD issue of how to manage business work product without breaching private personal data and information.

3.1.3 Mobile Content Management

Mobile content management (MCM) is the third layer that is needed to manage a BYOD enterprise level environment. Content is where users are very much hands on. For corporate managers, it is important that the content users access is in an environment that is secure and accessible, while offering the ability to share and collaborate. Mobile workers not only want but need to access the most current business documents and content quickly, anytime and anywhere, without worrying about

security risks. This security employs a variety of authorization and access permissions. These may include user authentication by logging-in to the system as well as entering authentication codes for particular documents.

Since mobile workers are not necessarily located at a fixed site, content may be dynamic depending on the worker's location through the use of a global positioning system (GPS) or navigation system. AirWatch's MCM application is called AirWatch Secure Content Locker; this is a secure centralized storage for all business content, files, and documents with three storage options. The cloud storage option can integrate with the most popular repositories such as Google Drive, Office 365, SkyDrive, and Amazon EC2. The on-premise option can integrate with the host repositories as well as a secure access to SharePoint without a VPN connection (AirWatch, 2013). The third is the hybrid option of the cloud and on-premise. AirWatch's MCM also facilitates two-way synchronization of content from users' desktops to mobile devices. So individual, user-created content can be accessible to any device that user owns. This option is exactly what the mobile worker needs and expects when working within a mobile-first environment. Again, the expectation is that these documents are always available with any device that is used to call it.

3.2 BYOD – A Decision Framework

The serious challenges in developing a BYOD strategy and the consecutive framework for its implementation is the impact BYOD can have on individuals' privacy, organizational security, and the liability of both entities. The Gartner analysts Andy and Nick Jones in their Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices have analysed and defined a structured approach in seven phases on the road to this emerging trend (Rowsell-Jones, 2012).

For corporate IT structures embracing a BYOD framework, the following key steps should be considered:

- Reasoning and deciding on a BYOD strategy – identify corporate mobile needs; define BYOD scope; shape sponsors' and stakeholders' commitments and responses to a BYOD program
- Design BYOD program segmentation by roles/needs/functions in the organization – categorize internal and external support, the range and type of access, and create packages of Policies and Technologies for each group
- Plan BYOD implementation by streamlining tools and technologies, network infrastructure and services, financing models, and exit options such as:
  - classify and approve list of devices and versions of mobile operating systems, applications, and providers;
  - design uniform policies, to enable scalable control and management of the user-owned mobile device utilizing Mobile Device Management (MDM), Mobile Applications Management (MAM), and Mobile Content/Document Management (MCM) solutions;
  - acceptable use policy with user's responsibilities and organization's rights against user's possession;
  - reimbursement plan options, total cost of ownership, corporate/private ownership separation, and list of approved exit options.
- Program setup and approval – complete internal policy, procedures, contracts, agreements, and training documents; educate stakeholders and ensure their sign-off; gain sponsors' budget and program approval
- Perform proof of concept by running a pilot over selected BYOD segmentations – modify procedure/policy/technologies based on the feedback and lessons learned from the pilot
- Program execution and evolution – periodic review and update of the BYOD program with current software versions, devices, applications, and providers. Utilize and evolve a mobile systems' features/limitations framework that supports the adopted corporate mobile management system(s).

The early BYOD adoptions have already experienced numerous concerns regarding losing personal data and privacy as corporations took full control over personal devices, applications, and information by utilizing mobile device management and device-level layer 3 VPNs. To address most of those critical anxieties, instead of a full control of the personal device, most corporations currently focus on adopting a set of tools to enable IT departments to wrap corporate applications in a security layer and to make sure that the enterprise control on the personally-owned device is limited only to the corporate data and applications. This actually shifts from MDM to MAM and from device-level VPNs to explicit application-specific VPNs involving technologies such as BIG-IP, APM, AppTunnels and encrypted connection to specific

service supported by Microsoft Exchange (Silva, 2012).

3.3 Assessing and Evolving BYOD

Based on the analysis and the framework outlined in the previous sections, a multidimensional approach for assessing the critical phases of BYOD policy implementation can be suggested:

- Risk Analysis to validate the strength of the BYOD policy; the following four key factors should be considered:
  - Social Experience – customers' and employees' satisfaction
  - Operational Efficiency – business process continuity and evolution
  - Financial Viability – forming business metrics over the lifecycle of the BYOD program
  - Technical Practicality – risk avoidances and risk management: how to prevent mobile security threats, how to handle disastrous events.
- Legal Issues and Privacy Concerns – several possible scenarios can be adopted to allow companies to benefit from being BYOD friendly while properly balancing the company's data security and compliance needs with employee preferences and concerns. The most common choices can include:
  - Mobile user utilizes personal smartphone for personal and work purposes. The company uses written contracts and MDM solutions that offer employees device flexibility and optimal network access in exchange for giving up some control over their personal devices. The company owns the right to wipe out the corporate documents from the user's device in case it is lost or hacked. The personal information should be guaranteed not to be erased or modified by the company's reaction.
  - The company owns the devices and enables employees to use them for both work and personal purposes – this trend is known as COPE (company-owned, personally-enabled). All information on that device can be erased or modified any time according to corporate rules and regulations.
  - Limited network access and data storage abilities in order to improve data security and employee privacy. This approach eliminates the need to utilize MDM; instead MAM or MCM would be recommended options to enable secure access to corporate data (Finneran and Brashear, 2014).

For any of the above cases, the BYOD program should apply concurring containerization, separate interfaces for corporate and personal data, special settings for data syncing and backup, and supplementing device-level encryption for enhancing corporate data security.

4 CONCLUSIONS

The current generation of mobile users demand a high quality wireless experience all of the time. Mobile workers depend on it and when it is not delivered as expected, productivity drops, ultimately costing company efficiency, profits, and brand reputation. Therefore, the paper discusses the needs, the decision framework, and the quality of user experience to be at the heart of any BYOD strategy. The adopted corporate framework has to provide a consistent, predictable, frequently updated, and secure experience for all users of the utilized mobile platforms, devices, and/or applications.

Further work is planned in two directions: how consumerization of IT is aligning to the current business strategies and operation models, and how carriers' 3G and 4G infrastructures and vendor's specific mobile platforms operationally and functionally impact the consumerization of IT at the enterprises.

REFERENCES

AirWatch, 2013. *Mobile Content Management: Top 10 Considerations*, Atlanta, GA, USA. Retrieved on 4/1/2014 from: http://www.air-watch.com/downloads/resources/white-paper-mobile-content-management.pdf

Appcelerator, Inc., 2013 *State of the Mobile Enterprise – Q1 2013 Mobile Enterprise Report,* Retrieved on 02/1/2014 from: https://www.appcelerator.com/enterprise/resource-center/research/q1-2013-mobile-enterprise-report/

ComputerworldUK, 2012. *BYOD Makes Employees Work Extra 20 Hours Unpaid*. Retrieved on July 1, 2013 from: http://www.computerworlduk.com/news/mobile-wireless/3377143/byod-makes-employees-work-extra-20-hours-unpaid/

Finneran, M., Brashear, J., 2014. *A Legal Perspective of BYOD: Building Awareness to Enable BYOD and Mitigate its Risk*, ZixCorp. Retrieved on March 25, 2014 from: http://go.zixcorp.com/rs/zixcorp/images/Zix%20Ebook_A%20Legal%20Perspective%20of%20BYOD.pdf

Forrester Consulting, 2013. *Exploring Business and IT Friction: Myths and Realities*, Cambridge, MA, USA

International Data Corporation IDC, 2012. *Worldwide Mobile Worker Population 2009-2013 Forecast and Worldwide Mobile Enterprise Management Software 2012-2016 Forecast and Analysis and 2011 Vendor Shares*, Retrieved on June 28, 2013 from: http://www.gotomypc.com/remote_access/images/pdf/How_to_Equip_Your_Company_for_the_New_Mobile_Workforce.pdf

iPass Inc., 2013. *The Enterprise Mobility Guide for IT Management and CIOs*, The iPass/MobileIron Mobile Enterprise Report, Redwood Shores, CA, USA

MobileIron, 2014. *Mobile Application Management*. Retrieved on 3/29/2014 from: http://www.mobileiron.com/en/solutions/mobile-application-management

Rowsell-Jones, Andy, Jones, Nick. 2012 *Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices,* Gartner, June 18, 2012, ID: G000234127

Silva, Peter, 2012. *BYOD 2.0: Moving Beyond MDM,* F5 White Paper. Retrieved on 09/20/2013 from: http:// www.f5.com/pdf/white-papers/big-ip-apm-mobile-application-manager-white-paper.pdf