Capgemini Consulting

Bring Your Own Device
It's all about Employee Satisfaction and Productivity, not Costs!

Abstract

> *BYOD questions how IT is viewed and implemented, and requires significant evolution in IT organization.*

BYOD is becoming more popular globally. For instance, a survey indicated that about 28% of the global workforce in 2011 used personal devices for official purposes[i]. This growth of BYOD is creating doubts in the minds of CIOs. Most focus on BYOD has primarily been from a cost savings perspective, however, our analysis indicates there are more important reasons for CIOs to consider.

When employees use personal devices at the workplace, businesses clearly save on capital expenditure of hardware and software, and related IT operational expenses. But cost benefits often get eroded by further investments such as virtualization or security reinforcement to support the BYOD model. With such long-term sustained investments, it appears BYOD doesn't have a significant cost advantage. The business benefits, instead, appear to lie elsewhere – one of the major benefits of BYOD is employee satisfaction. In addition, it boosts employee mobility, productivity and is perceived as a strong differentiator in attracting talent. The satisfaction among end users can also be leveraged to strengthen IT department's image. Organizations need to recognize and respond to the BYOD trend quickly to leverage new opportunities presented in terms of increased employee satisfaction, mobility and productivity.

However, BYOD is not a simple IT project. It questions how IT is viewed and implemented, and requires significant evolution in IT organization to promote service-oriented models. It is critical for organizations to analyze key factors related to security policies, delivery model, IT solutions and support structure in order to define a successful customized device-agnostic BYOD strategy.

There is No Clear Business Case for BYOD

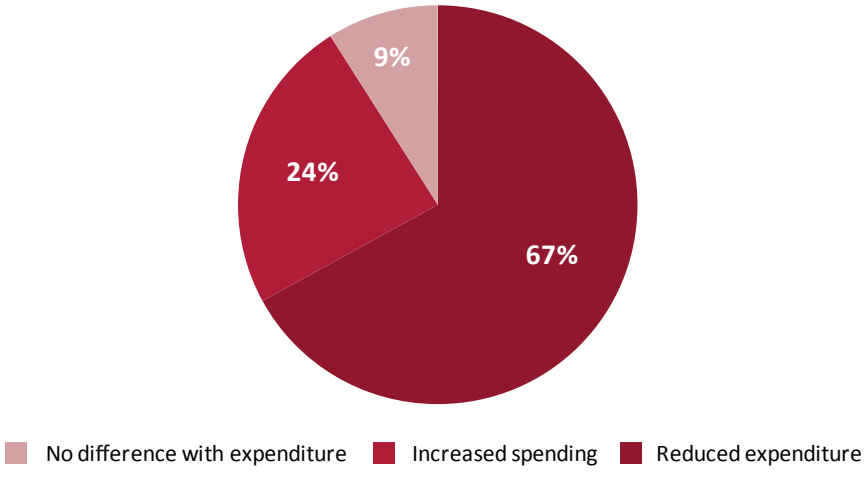
Bring Your Own Device, or BYOD is a concept by which organizations allow employees to connect their personal devices, such as laptop, tablet and Smartphone, to the corporate network, so that they can access business and collaborative applications.

The driving belief behind BYOD adoption is that companies benefit by saving capital costs as they no longer have to provide employees with computing devices or related software. However, a BYOD initiative need not always be cost effective, especially since additional investments are needed to support the usage of personal devices in a business environment. For instance, a study found that only 9% of organizations have been able to reduce expenditure by deploying some kind of BYOD program[ii] (See Figure 1).

Considering basic costs under a BYOD model, our own analysis of total cost of ownership (TCO) has shown that TCO in a BYOD arrangement is only 9.7% lower than that of a standard model (See Figure 2)[1]. However, when additional cost heads are factored in, BYOD fails to demonstrate a clear cost savings advantage. These cost heads can vary substantially from one organization to another based on multiple parameters such as existing IT set-up, number of BYOD users, type of delivery model selected and platforms to be supported.

"Only 9% of organizations have been able to cut expenditure by deploying some kind of BYOD program while 67% saw no difference with expenditure."

Figure 1: Percentage of Respondents According to Impact of BYOD on Expenditure (2012), North America

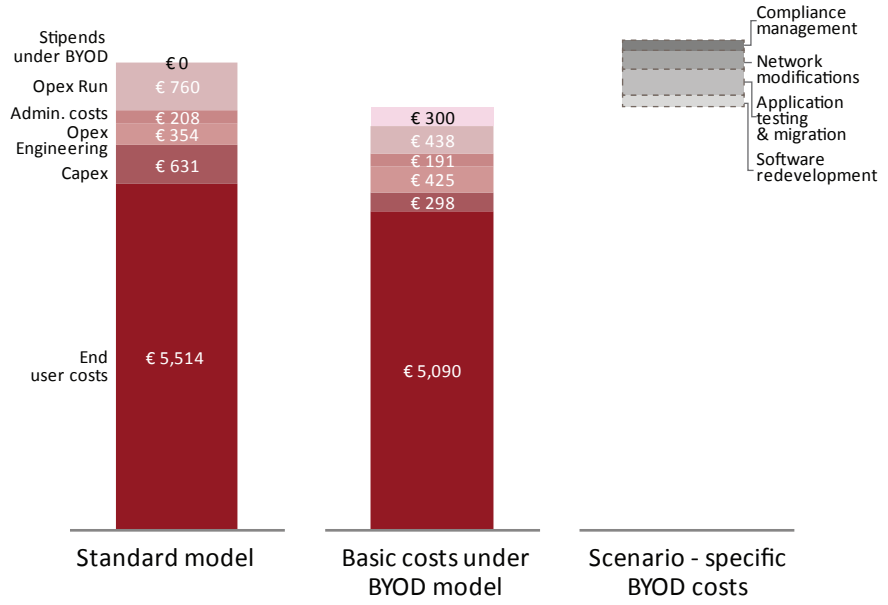


Source: Xigo and CCMI Research (North America), July 2012

[1]*The TCO analysis is based on the calculation for 2,500 traveling workforce in a centralized IT organization. The traveling workforce is assumed to work outside the traditional office environment 80% of the time and use unmanaged notebooks. Moreover, full implementation has been considered under BYOD model (device virtualization), wherein employee sources as well as maintains a device and related software.*

When additional cost heads are factored in, BYOD fails to demonstrate a clear cost savings advantage.

Figure 2: Total Cost of Ownership Analysis Indicating Unclear Cost Benefits of BYOD Model



Source: Desktop and Laptop Total Cost of Ownership, Gartner, 2011; Capgemini Consulting
Note: Cost heads are further explained in the endnote (See Reference section)

These cost heads include software redevelopment to support multiple mobile platforms, application testing and migration, building wireless and virtual private network infrastructure, and compliance management. Take the instance of data plans: in a BYOD model, companies can no longer negotiate corporate or group discounts for devices, services and data plans, and paying for a large number of individual subscription plans is almost always more expensive than a bundled service contract[iii]. While they might be nominal costs individually, collectively they have the potential to adversely impact the realizable TCO benefits from a BYOD arrangement. For instance, when 600 workers at a technology company joined a BYOD Smartphone program, expenses exceeded the budget in the first year by over $300,000[iv].

Cost savings are certainly not the main driving factor for BYOD adoption. So, why should organizations continue to adopt BYOD? Employee satisfaction and enterprise mobility remain two of the biggest drivers for BYOD adoption. Since enterprise mobility promises enhanced employee productivity, organizations are foreseeing potential for revenues. In the next section, we will discuss these benefits in more detail.

Business Agility Drives BYOD, Not Costs

> *19% of businesses perceived BYOD as a way to enable employee satisfaction, while 17% felt BYOD could improve productivity at the workplace.*

Major Benefits of BYOD

The major benefits from BYOD include improved employee convenience and satisfaction, increased employee productivity, greater workforce mobility and employee retention as well as higher agility in business operations (see Figure 3).

First, in a BYOD environment, employees do not have to carry multiple devices or switch between personal and work devices. In addition, employees feel more comfortable while working on personal devices, which improve their job satisfaction levels. According to a survey, 19% of businesses perceived BYOD as a way to enable employee satisfaction, while 17% felt BYOD could improve productivity at the workplace[v]. For instance, by allowing employees to use their personal Smartphones and iPads, Cisco registered a 33% increase in employee satisfaction, even though the company did not pay for these devices or service plans[vi].

Figure 3: Major Benefits of BYOD

Source: Capgemini Consulting

Second, a BYOD model leads to changes in employee work habits. It enables employees to use their devices after work hours or during 'out of office' periods to deal with basic tasks, which reduces wait times and enables quicker resolution of action items. Shorter turnaround times and seamless business operations drive business productivity. For instance, a survey among mobile workers showed that workers who use mobile devices for both work and personal purposes put in 240 more hours per year than those who do not[vii].

Third, extended connectivity through mobile devices and remote access to the corporate network offers employees greater mobility. Moreover, mobile services on employee-owned devices enable employees to collaborate in real time and efficiently execute tasks irrespective of their location or time zone.

Further, offering employees flexibility in device selection is an incentive for existing as well as prospective employees. It also communicates the message to the workforce that the organization trusts its employees in making their own decisions about how they work. Thus, with effective implementation, BYOD can act as an important tool for attracting and retaining talented people. Also, managed personal devices and application virtualization enable seamless connectivity to corporate data under a BYOD environment, thereby enhancing overall business agility.

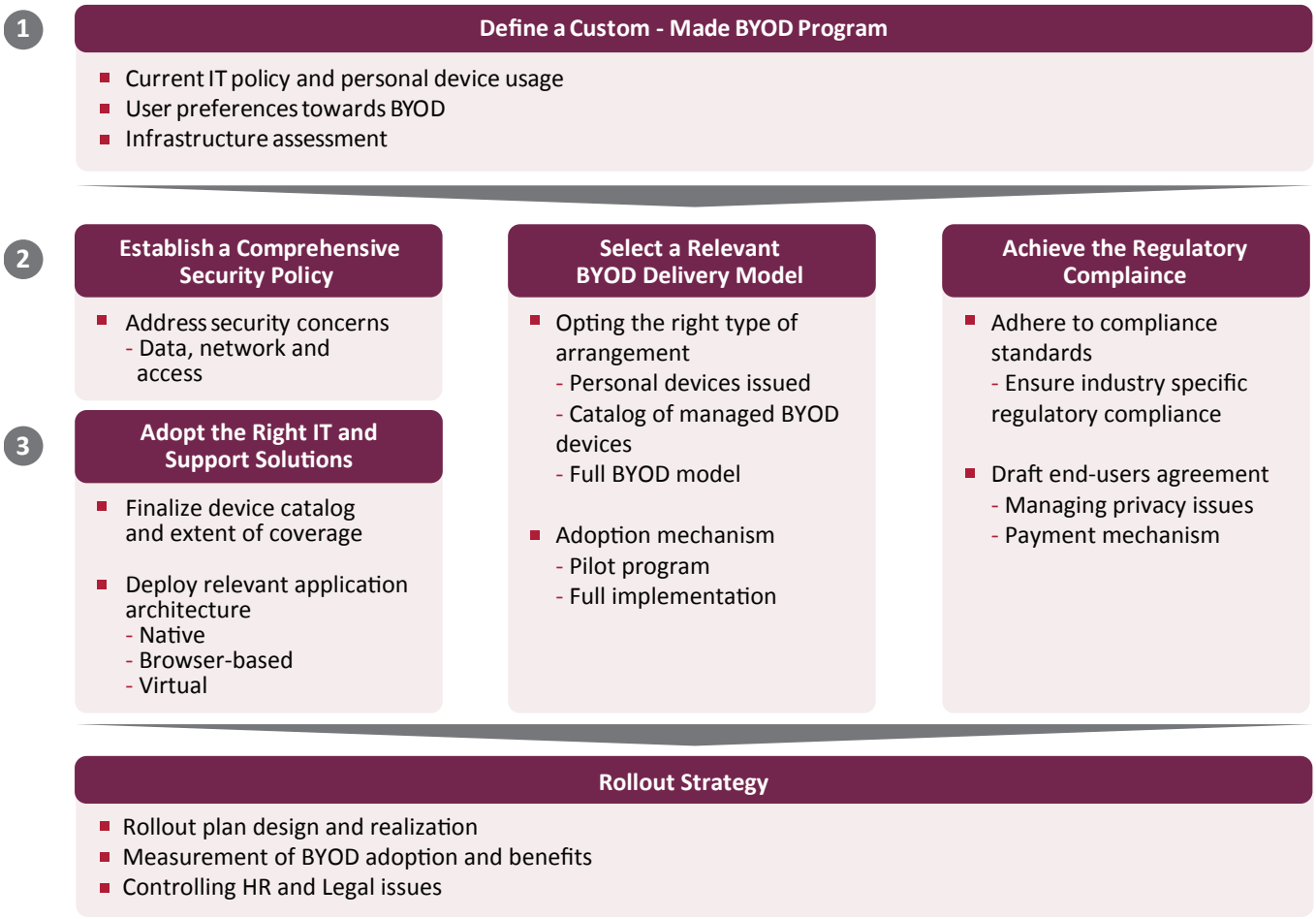
So, improved employee satisfaction and business agility through BYOD is clearly a productive endeavor. But without a comprehensive strategy, policies and technology in place, BYOD exposes companies to increased costs, security risks and operational issues. In the subsequent section, we will describe key factors essential in drafting an effective BYOD strategy and discuss the related implementation roadmap.

> *"Mobile workers who use mobile devices for both work and personal purposes put in 240 more hours per year than those who do not."*

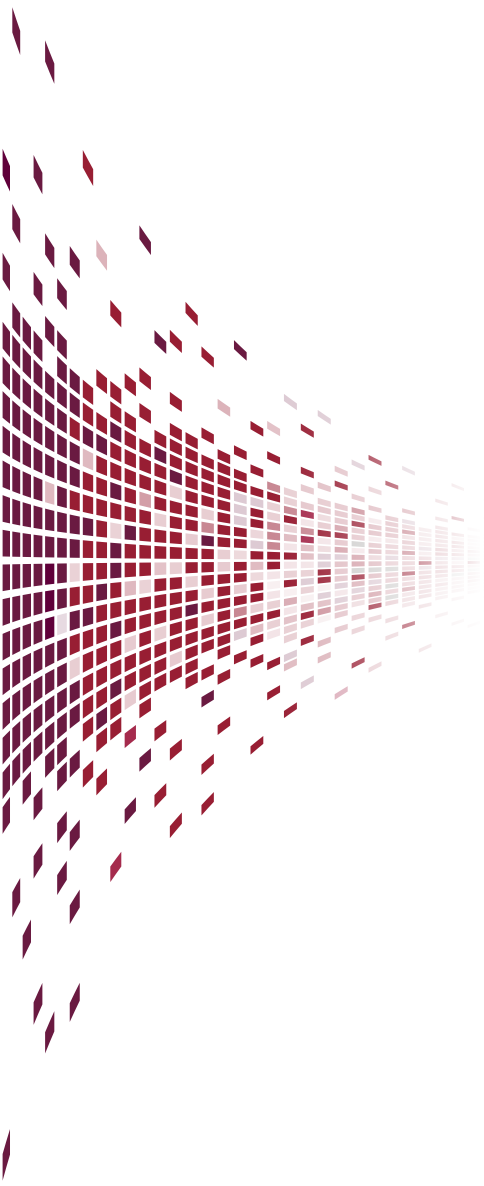
Roadmap to BYOD Implementation

A BYOD implementation entails new procedures, metrics, and organizational structures along with IT architectural flexibility. We have developed a BYOD implementation framework along with crucial factors to roll out an effective BYOD strategy. Such a strategy would involve defining a customized BYOD program, establishing a comprehensive BYOD policy, selecting the right BYOD model, and adopting relevant IT and support systems, followed by a rollout strategy (see Figure 4).

Figure 4: BYOD Implementation Framework



Source: Capgemini Consulting



1. Define a Custom-Made BYOD Program

The definition phase involves infrastructure assessment and evaluation of current states. A review of current IT policy is crucial to determine types of personal devices allowed and levels of access provided for business applications from these devices.

Moreover, internal surveys conducted across an organization can reveal aspects such as employee opinions and interest towards BYOD programs, expectations such as compensation and support from the organization, and device-specific preferences. This will result in a realistic assessment of the feasibility of the BYOD program in the organization, and of end-user expectations during the initial stages of BYOD adoption.

Infrastructure Assessment

A review of current network architecture, including arrangement of firewalls, network policies, datacenter scalability, network and end-point visibility, is essential to understand BYOD associated risks. Key infrastructure-related questions to be considered while framing an effective BYOD strategy are whether the organization has real-time control of content and user activity, which applications and data are potentially exposed to security risk, and if existing infrastructure is capable of handling increasing personal device usage.

Segmentation of End Users

Organizations need to identify employee eligibility towards a BYOD model after assessing risks pertaining to sensitive corporate information. While some groups of employees have a strong BYOD requirement, other groups may not necessarily be well-suited to a BYOD model. For instance, as many as 62% companies actively target the mobile workforce when implementing a global BYOD model [viii].

> *As many as 62% companies actively target the mobile workforce when implementing a global BYOD model.*

2a. Establish a Comprehensive Security Policy

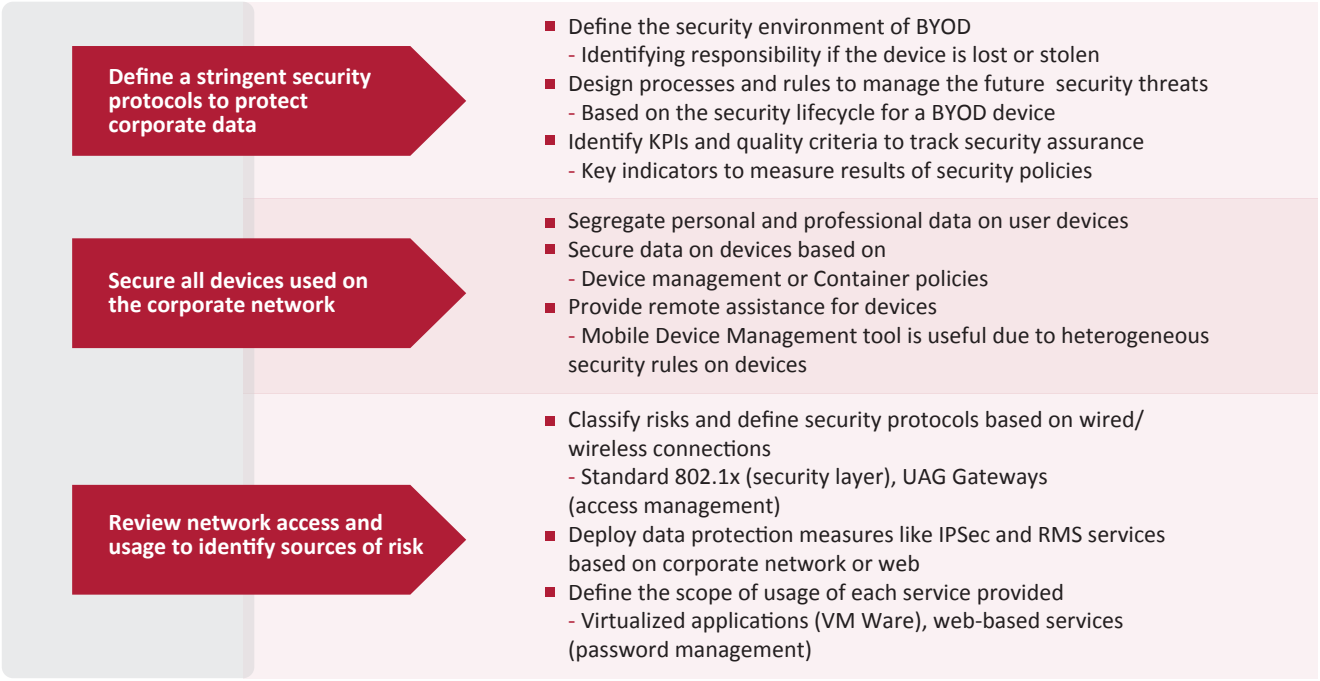
The freedom to use personal devices at work alters the traditional structure and scope of control of the IT department. Understanding the modified environment will provide organizations with greater clarity on what to consider when drafting BYOD policies. The organization also needs to clearly prescribe specific courses of action in the event of policy guideline violation.

Mobility and IT consumerization present evolving, complex security threats that require redesigning existing security strategies. As Figure 5 illustrates, this strategy can be implemented through specific action points.

Since sensitive organization data are stored on employee-owned devices, BYOD brings its own security concerns. So device security management needs to be strictly enforced. Moreover, BYOD requires a new control framework as security enforcement is not just limited to devices. Organizations need to adopt a systematic globalized security approach that encompasses data, hardware, software and network. Security rules based on device management or container policies have to be defined for each category (laptop, tablet, Smartphone) of BYOD devices.

Further, the risk of data being compromised from a lost or stolen device is one of the major security challenges faced by organizations when dealing with a BYOD program. Businesses need to chart a clear plan and use relevant mobile device and application management solutions to deal with lost or stolen devices. The plan need to include clear notification process, necessary steps to be taken to remove access to the corporate network and procedure to remotely erase local data stored on the missing device.

Figure 5: Major Action Points to Overcome Security Concerns Presented by BYOD



Source: Capgemini Consulting

2b. Adopt the Right IT and Support Solutions

A cross-analysis of the end-user segmentation, type of personal device used and business application accessed, allows organizations to develop a relevant IT solution. It is important to finalize device catalogs and deploy the relevant application strategies to develop an agile infrastructure for a BYOD environment. The first step is to finalize the device catalog and extent of device coverage. A BYOD model entails a transformation of the device catalog list from a limited number of supported platforms to a much wider list. Companies need to decide if they would allow all personal devices or specific device categories such as laptop, Smartphone and tablet on the corporate network.

The second step is to deploy the relevant application architecture, ranging from virtualization software such as VMWare and XenApp, to browser-based access, to server-based computing and hosted virtual desktops. Further, creating a central repository of enterprise software under the BYOD arrangement would enable employees to easily access and download the software, as and when needed (see Needham Bank's Case Study).

Finally, a corporate app store under a BYOD environment can offer employees the freedom to select the software they require on their device without the typical service desk intervention. The creation of a corporate app store will also reduce IT helpdesk costs. For instance, a study found that 12% of IT helpdesk ticket requests are for new software installation, and it is estimated that a corporate store can potentially save over $8.6 million a year in IT helpdesk costs[ix].

> *A study found that 12% of IT helpdesk ticket requests are for new software installation, and it is estimated that a corporate store can potentially save over $8.6 million a year in IT helpdesk costs.*

Needham Bank's Case Study

Needham Bank deployed remote desktop solution to enhance worker productivity through BYOD

Background

Needham Bank, a US-based community bank, needed to provide its employees an access to range of bank's applications from mobile device to increase bank's overall productivity levels during evenings and weekends. Meeting security and compliance norms set forth by government regulations were the key considerations in evaluating a feasible solution.

Initiative

In order to enable mobile access, Needham Bank provides some employees iPhones and iPads (based on eligibility-criteria), which the company manages. Other employees, who do not qualify for company-owned devices, are allowed to use their personal devices for work. Using single sign-on credentials bank employees can remotely log into their office devices from any device to access key applications.

To address security concerns, the bank uses mobile device management solution and train workers on following safe practices while using own devices. The bank also blocks its employees from downloading apps like Dropbox, a cloud storage service, and from using iCloud, Apple's storage service. The bank's IT also restricts printing and clipboard functions to prevent data leakage. In addition, the remote access solution keeps the data 'off-the-network' and no data or files are stored on iPad or remote devices, so there is no threat to sensitive data in case these devices are lost or stolen.

Benefits

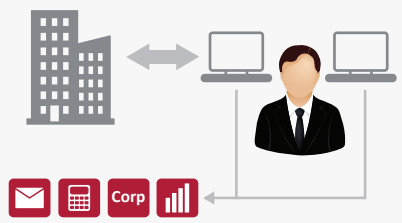
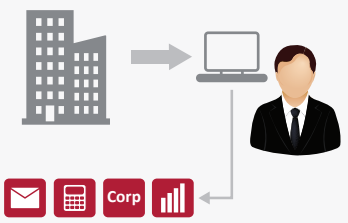
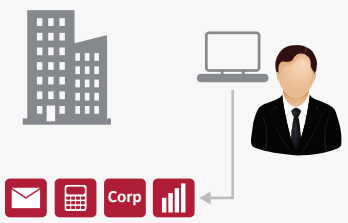
Through remote and mobile access, Needham Bank achieved significant increase in productivity due to streamlining of operations, eliminated the potential of data leakage and enabled employees to use their device of choice for work. For instance, Bank's accounting team can quickly access financial data remotely while the business development team can access core banking applications to get relevant account and relationship information right before going into client meetings. Since, implementation of this initiative, Bank has recorded increase in number of remote and mobile users by 11 times while time spend working remotely has grown by 120 times, driving overall business productivity of Needham Bank.

Source: Banks May Not Be Able to Resist BYOD, InformationWeek, April, 2012; Array Networks, March 2012

2c. Select the Relevant BYOD Delivery Model

The BYOD delivery model needs to be selected based on the industry, IT maturity level, organization structure, partner ecosystem and regulatory guidelines in the region of operation. Figure 6 illustrates three types of BYOD delivery models, with corresponding infrastructure layouts and support structures, based on end-user device ownership. Selection out of these delivery models depends on employees' needs in terms of security, access to applications, device preferences and need for mobility.

Figure 6: Three BYOD Models Based on Computing Device Ownership, Infrastructure Set-Up and Support Policies

	Personal devices issued	Catalog of managed BYOD devices	Full BYOD model
			
End Users	▪ Work with the company owned workstation and their personal device	▪ Own their workstation sourced from within a company service catalog	▪ Source and own their workstation
Infrastructure and Applications	▪ Partially virtualized - IT sources workstations without employee involvement - Emails and some business apps are made accessible on personal devices	▪ Well virtualized - IT offers a device catalog and lets employees choose their devices - All services and apps are available on the employee's own workstation	▪ Well virtualized - IT may offer allowances to employees for purchasing the device - All services and apps are available on the employee's own workstation
Helpdesk /Support	▪ IT supports company workstation and corporate services available on personal devices	▪ IT supports employee's own workstation including all services on it	▪ IT only supports business apps and exchange services (collaborative tools) ▪ Support for the hardware, device and basic services (OS, office apps and browsers) is the employee's responsibility

Source: Capgemini Consulting

Ford Motors Case Study

Ford Motors adopted a user community-driven approach to control support costs under BYOD program

Background

Ford Motors, a leading US-based automaker, started a program called 'Digital Worker' back in 2007, which looked at all collaboration tools to drive increased capability globally. Out of the four core areas identified for this program, mobility solution including BYOD was a key focus area. The company then created a cross-functional team consisting of managers from the IT, legal, HR, accounting and other departments to examine the risks and rewards of BYOD.

Initiative

In 2009, Ford rolled-out a corporate-liable program (CLP) to enhance employee convenience and productivity. Under CLP, company provides devices, pays for the service and offer help desk support to the employees for whom mobility is critical. However, with the increasing number of users and to control capital costs, company decided to launch an alternative individual-liable program (ILP). Termed as email on Personally Owned Devices or ePOD, the program enabled employees to access corporate emails on personal devices. The structure of this program is that – employee pay for the device and data plans. The support model is self and user community driven, wherein a group of BYOD users interact on common online platform to resolve BYOD related queries and issues. The company bears the back-end costs of servers and software licenses such as Mobile Device Management.

The employees would fit into a corporate-liable (company-owned devices) or individual-liable (personal devices) program based on their job requirement and business criticality. Employees under BYOD would sign a participation agreement, so that they clearly understand their roles and responsibilities, what is the support model, who pays what costs and other conditions of the program.

Benefits

The BYOD program resulted in increased flexibility for Ford employees with seamless integration of personal and work activities as well as reduced costs associated with enterprise mobility functions. From initial 2,700 subscribers under BYOD (ILP), the program has been expanded to include over 70,000 employees in 20 countries. The company recently deployed new mobile security system and included other business applications in addition to access to corporate email through Smartphone, tablets and other mobile devices.

Source: How Ford Motors Deployed BYOD, Forbes, July 2011; SearchCIO.com, August-September 2011

2d. Achieve the Regulatory Compliance

Organizations devising a BYOD framework should not only ensure that the policies are acceptable to employees but also that they address all statutory requirements regarding compliance and tax legislations. The BYOD model should be regulatory compliant with norms such as Health Insurance Portability and Accountability Act (HIPAA) for healthcare segment, and Payment Card Industry Data Security Standard (PCI DSS) for financial services sector, regardless of the device on which data is stored. It is also important to draft guidelines and agreements pertaining to end-user privacy issues since professional and personal tasks would be carried out on a same employee-owned device. Employees eligible for BYOD need to accept and sign an agreement. The agreement explains how the organization intends to treat corporate and personal data and communications on the employee-owned device along with device and support compensation terms.

Further, organizations need to have tiers of compensation policy (no compensation, limited compensation or full reimbursement) for expenses towards devices, data plans and support. A survey across 17 countries reported that 55% of employees pay for at least one device they use for work purposes[x] (see Ford Motors Case Study).

3. Rollout Strategy

The rollout strategy entails designing the plan, guiding employees about BYOD to help them decide whether to join BYOD program, understand cost subsidies, if any, as well as how data would be accessed, used and stored on personal devices. The organization can choose to adopt a company-wide BYOD rollout mechanism or approach it in a phased manner.

Conducting regular audits of personal devices ensures that employees abide by the BYOD policy. Measuring benefits of BYOD, such as improvement in productivity and employee satisfaction, enables organizations to alter the BYOD program accordingly. BYOD presents risks in managing work conditions, device warranty, taxation impact, and support desk usage by an employee. While implementing a BYOD model, all associated social and legal risks need to be analyzed to avoid potential HR and legal issues. Further, the implementation of BYOD model needs to have a strong review and measurement process to keep track of the benefits, challenges and future actionable points.

The funding responsibility to promote BYOD initiative can be transferred to the business units instead of corporate IT budgets. Such arrangement would distribute the cost burden as well as accountability for success of BYOD program to individual business units. We believe that BYOD model should be considered for creating business value that goes beyond cost savings.

Growing expectations around usage of employee's personal devices at the workplace indicate clearly that the BYOD trend is here to stay. By encouraging employees to use personal devices, BYOD policies not only boost employee satisfaction and drive business productivity, they also help organizations become nimble. An effective BYOD policy can help organizations integrate, and encourage, greater usage of digital tools. As digitization and the imperative to digitally transform become more critical, BYOD policies can be leveraged successfully to gain employee acceptance and buy-in for large-scale transformation programs.

> *"A survey across 17 countries reported that 55% of employees pay for at least one device they use for work purposes."*

References

i IT Organization Embrace Bring Your Own Devices, Citrix, 2011

ii Mobility Temperature Check: Just How Hot Is BYOD?, Xigo and CCMI, July 2012

iii Asian companies resisting BYOD due to cost, ZDNet, November 2012

iv BYOD Planning and Costs: Everything You Need to Know, CIO.com, December 2012

v Survey of telecommunication professionals in North America, Xigo CCMI, July, 2012

vi What is the business value in employees "bringing their own device" into the workplace?, Cisco Service Dynamics, 2011

vii 5 Things You Need to Know about BYO Tech, CIO.com and iPass, December 2010

viii Global BYO Index, Citrix 2011

ix Corporate App Stores: Harness The Power Of BYOD, Forbes and 1E, March 2012

x Charting the Rising Tide of Bring-Your-Own-Technology, Forrester, June 2012

Note on Cost heads considered for TCO analysis of BYOD and standard model

Capex: Cost of ownership for hardware (laptop, server) and software (OS) decreases as employees bring their own device. However centralized architecture such as server-based computing or hosted virtual desktop would require additional investment in server infrastructure.

Opex Engineering: Security management costs would increase in the BYOD arrangement and desktop management (fleet deployment, replacements, outsourcing) expenses will reduce moderately or remain constant.

Admin. Costs: Although IT disposal costs decreases under BYOD environment, IT training cost increases with new device management and application access processes.

Opex Run: Virtualization and transformation into web based application decreases hardware and software maintenance costs under BYOD. But cost of ownership and maintenance for IT-specific software, Tier 1 IT support (password issue, application access issue) and data center storage costs would increase due to complex security deployment in the BYOD arrangement. Tier 2 and 3 IT support will come down as devices are owned by employees.

Stipends under BYOD: Grants for purchase of end user device and its support based on the BYOD model and compensation policy adopted by the company.

End-user Costs: End-user training decreases as employees are familiar with their devices and software as well as extra costs due to downtime of end-user IT equipments reduces.

Authors

Benjamin Alleau
Vice-President
benjamin.alleau@capgemini.com

Johann Desemery
Principal
johann.desemery@capgemini.com

*The authors would also like to acknowledge the contributions of **Jerome Buvat** and **Vishal Clerk** from the **Digital Transformation Research Institute** of Capgemini Consulting.*

For more information contact

DACH
Guido Kamann
guido.kamann@capgemini.com

Netherlands
Eric Kruidhof
eric.kruidhof@capgemini.com

Spain
Christophe Jean Marc Mario
christophe.mario@capgemini.com

France
Cyril Francois
cyril.francois@capgemini.com

North America
Martin A Hanlon
martin.a.hanlon@capgemini.com

Sweden/ Finland
Ulf Larson
ulf.larson@capgemini.com

Middle East
Jawad Shaikh
jawad.shaikh@capgemini.com

Norway
Gunnar Deinboll
gunnar.deinboll@capgemini.com

UK
Stephen Pumphrey
stephen.pumphrey@capgemini.com

Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Find out more at:
http://www.capgemini-consulting.com/

About Capgemini

With around 120,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2011 global revenues of EUR 9.7 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us
at www.capgemini.com.