Volume 4, No. 4, April 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES

[1]Prashant Kumar Gajar, [2*]Arnab Ghosh and [3]Shashikant Rai
[1]Master of Science-Cyber Law & Information Security
Indian Institute of Information Technology-Allahabad India
prashant.developer@gmail.com
[2*]Master of Science-Cyber Law & Information Security
Indian Institute of Information Technology-Allahabad India
arnabghosh.ghosharnab@gmail.com
[3]Master of Science-Cyber Law & Information Security
Indian Institute of Information Technology-Allahabad India
shashikant@iiita.ac.in

Abstract: The growth of mobile technology, with regard to availability of 3G/4G services and devices like Smartphone's has created new phenomenon for communication and data processing ability to do business. One such phenomenon that has emerged in the business environment is BYOD (Bring Your Own Device), which means that employees use their personal device to access company resources for work, inside or outside organizational environment. This new phenomenon brings with itself new opportunities but has many risks associated with it. Using mobile devices for personal as well as professional work brings with itself risks that need to be mitigated. The aim of this work is to provide various mobility strategies, defences and measures, control aspect, management and governance aspect to look forth in implementing a BYOD strategy in an organization.

Keywords: Risk, Defences, Bring Your Own Device, Have Your Own Device, Choose Your Own Device, Here is Your Own Device, Mobile Device Management, Control Objective, Controls and Governance

INTRODUCTION

BYOD is a brand new concept emerging in the industry which facilitates employees in the organization to use their personal mobile devices to access the resources of the company for both work as well as personal use. Tasks may range from accessing corporate e-mails, documents, applications and network etc. In 2009, the concept first entered into the corporate scenario when Intel recognized the importance of employees using their own devices for accessing corporate resources and network [6]. But it was only until 2011 when IT service providers like Unisys and software vendor like Citrix Systems shared their views and perceptions about this emerging trend, organizations started considering it [7].

An employee seems to be highly dependent upon using any of their portable devices be it laptop, iPad, smart-phone or even a USB stick for their work purpose just because they find their devices much cooler than those provided at their cubicles or desk in an organization. By which we understand that to be competitive in the market, organizations need to facilitate any kind of technological advancement at the end user side which are their employees, but not compromising with the security of corporate information and privacy of end user [15].

Use of mobile devices popularity has increased which was not possible with the enhancement of:

Connectivity:

The mobile devices are can now be well connected to the corporate network through Wi-Fi`s. Hence they can always stay connected and access their resources.

Application access through web:

All the applications of the organization can be accessed through Web such as business, sales, customer support, finance, technology etc. Hence this single point information accessibility also reduced various technical requirements within a device.

Mobile device advancement:

An increase in the growth and development of mobile devices with vivid features and functionality has raised the bar to be used as an acceptable device within an organization. These devices are now more powerful and sophisticated and have performance very near to that of desktops. The increased security features within the device has also helped it in its acceptability [16].

The BYOD concept, is in itself bringing in a new idea of Bring Your Own Technology (BYOT) and Bring Your Own Software (BYOS) in which employees use non-corporate software and technology on their device. This increases the scope altogether for an employee to use its own technology, but in turn creates many challenges for the organization [13].

The figure below shows the statistics of the type of devices used by the employees in a survey conducted by Forrester`s Foresight's Workforce Employee Survey, Q4 2011 [8].

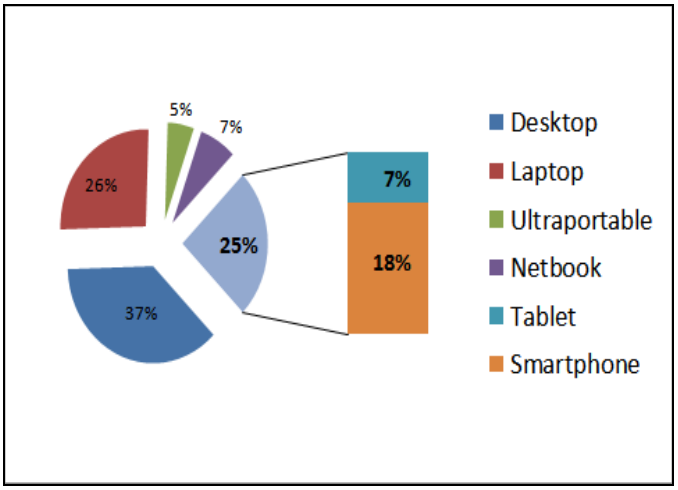

Figure 1: Devices used in a company. Source: Forrester`s Foresight's Workforce Employee Survey, Q4 2011.

BENIFITS

If we are talking about the benefits, BYOD concepts is really enhance the employee's functionality because due to implementation of BYOD concept the corporate information and organizations data is readily available to them on their personal devices likes smart-phones, PC's or laptops. Spending's of the organization are reduced considerably with regard to devices and procurement and training. There is increased productivity and efficiency of an employee in the organization and increases their morals. Also new devices will bring with them cutting edge technology generally owned by the employees. Using their own devices help employees to handle the device in an efficient manner as they are more familiar and comfortable with the functionalities of the device and also the capability for employees to be flexibly work form their home or on the road as per the their convenience. Also a using its own device means an employee will take an extra care for its safeguard. Since corporate information and personal information are on the same device, the ease of use to fetch information also enhances. Due to this the communication would be faster and efficient [14].

As per the trust in technology survey [3], 53 % of the corporate world officially approved and accept BYOD concept and its practice. In that total 53 %, 20% of subsidy to employees who already start using their own smart-phones, PCs or laptops in the organization for work purposes, which is exactly less than the traditionally any organization spend to acquire the same resources which is required for work purposes. And left out i.e. 33 % of the organizations allows BYOD, but do not subsidize it at all, so the savings are more significant [3].

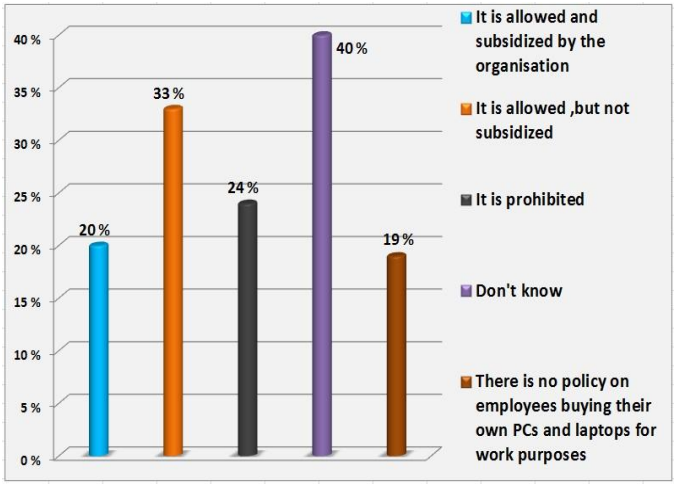

Figure 2: Organizations' policies on employees using their own personal computers or laptops for work purposes [3]

CHALLENGES

The extra portability of mobile devices pose a great challenge to the security of the device, along with the information on it as they can be very easily lost or stolen. Personal devices may not be sophisticated in terms of security such as anti-viruses, patches, firmware updates and configuration settings. Any unauthorized or non-business oriented applications have the potential to affect the integrity of the device and the business data residing upon it. Also mobile devices use variety of operating system and there are constant changes with technical advancement and get outdated very quickly. The devices can be jail broken. Controls are lacking with respect to device, security and data, due to lack of enterprise-strength security controls a range of mobile device platforms, such as BlackBerry, Symbian, IOS, Android and Windows Mobile, needs to be supported, and each platform bring with it a unique security model. Privacy of employee also an issue as devices stores numerous personal credentials and data.

The Business and personal data coexist on same device then it's very difficult to find a balance between a strict security control of enterprise and privacy of personal data, specifically when the device is no longer a corporate issued asset. Incident detection such as lost devices versus breached devise or actual versus suspected breach is also a problem. Confidential information is being sent or received over an unsecure channel. Many mobile devices are always on and connected, so the vulnerability to malicious attacks increases through different communication channels. Connecting rouge devices and access points with the help of device can also be problematic. Some human factors like a disgruntled employee may store confidential business data on his personal removable media and give this information to its competitor which may cause loss to the organization. Lastly complying with contracts, laws and even own policies may seem to be a challenge [12].

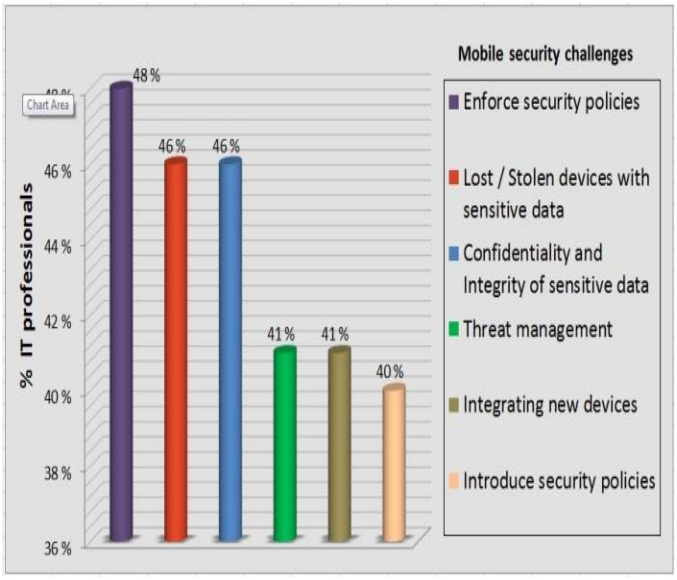

Figure 3: Challenges with mobile device. Source: ESG research survey [1].

RISK AND THREATS

Risks :-

- ***a. Credential Information:*** User credentials like username and Password, installed certificates, banking information, web accounts, and E-mail accounts can be accessible if the device is compromised or if it lost/stolen.
- ***b. Confidential Business Data:*** Confidential Business Data like Email, documents, Reports, files, Application etc. is at risk if unauthorized access of the device takes place due to device compromised.
- ***c. Phone and Data Services:*** There lies risk to eavesdropping on call or sniffing of packets, the device can get unauthorized access and device can be rooted or jail broken.
- ***d. The Device Itself:*** The device being highly portable, there lies a risk of getting it lost or stolen very easily.

Threats : -

- ***a. Malware:*** A compromise of device by malware can lead to loss of confidential business data or can use additional services like calling in the background and sending text messages. It can disrupt the working of an application or the whole device and make it unusable.
- ***b. Spam:*** Unsolicited messages and e-mails are received from known or unknown sources causing wastage of resources such as bandwidth and memory space.
- ***c. Phishing:*** Phishing is possible through an e-mail or SMS phishing to trick a user to access fake website to access business accounts.
- ***d. Bluetooth and Wi-Fi:*** Bluetooth and Wi-Fi can easily be used to infect mobile devices. A mobile device can be lured to accept a Bluetooth or Wi-Fi connection which can turn out to be malicious and can intercept all the data to or from the connected devices [18].

SECURITY STRATEGY FOR MITIGATING RISK IN BYOD ENVIRONMENT

Mobility strategy in an organization:

The following framework can be used by the organization for end user mobile computing that would help to define the security strategy for implementing BYOD.
The four concepts that come up are:

- ***a. Here is your own device (HYOD):*** In this concept, the devices are provided by the organization. There is total control on the device by the enterprise. The enterprise will provide the complete support for the device, starting from installation to configuration and settings etc. of the device.
- ***b. Choose Your Own Device (CYOD):*** In this type of strategy, the organization provides a number of devices, from which an employee can choose his own device to use. The policies are not so stringent as was the case with have your own device and the user has authority to install some specific apps and software.
- ***c. Bring Your Own Device (BYOD):*** The employee buys his device or the organization provides helps financially to buy their own device on which they want to work from consumer market. Here the policies are weaker and less control of organization on the device. User can do whatever they want like installing apps they want, if they are complying with the organization's policies. Some support with regard to configuring the device according to organization`s policies will be done.
- ***d. On Your Own Device (OYOD):*** The end user i.e. the employee can bring in any device on which no support will be provided by the organization. The user has the responsibility to manage the device. No policies are needed to be followed.

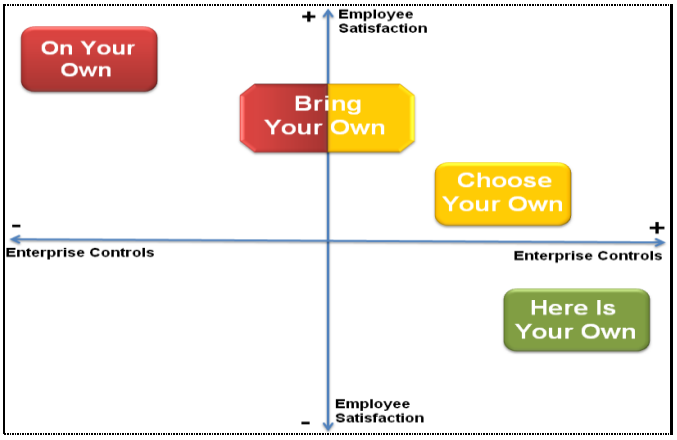

Figure 4: Enterprise Control v/s Employee Satisfaction map of various mobility strategies.

As per the above figure, Here Is Your Own Device style strategy although gives maximum enterprise strength security control but as the device is provided to the employee directly, he is remains with no power of choice to use a device of its liking, hence we see a considerably low employee satisfaction. With Choose Your Own Device, with enterprise giving option to choose from a set of devices, employee satisfaction increases to a greater extent, but there are stringent controls of

organization implemented. Bring Your Own Device strategy allows users to buy the devices of their own choice from the consumer market, increasing employee satisfaction and then apply some policies and controls on the device. The strategy free from organization`s control would be the On Your Own Device, where user can buy the device of their wish and control and manage the device the way they want. It increases the employee satisfaction to the maximum level.

But with the terminologies explained above the BYOD and OYOD fall under the category where the devices are bought by end-user from the consumer market. But in all the situations the organization has to give access to the employee to use its applications and data, which creates altogether different risks at different levels. It is a very clear fact that that, due to lack of controls on the devices of end-user, security issues would arise definitely, as the organization has to deal with too many heterogeneous devices in the organization, mixing their professional and personal work adding complexity and risk into the system, where as in a normal environment, the organization has to deal with small set of devices and operate in a standardized manner. So in a way some control strategies needed to be developed to address the issues of mitigating the risk, so that ways of accessing the resources can be made secure.

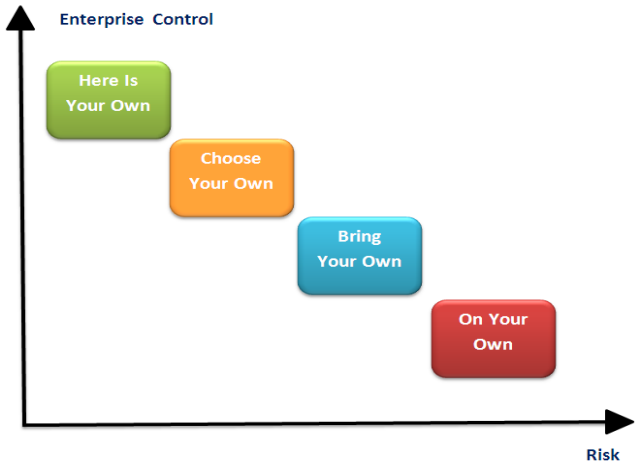

Figure 5: Risk v/s Control map of various mobility strategies.

Decide Best Approach:

The decision on the approach to go ahead with the mobility strategy will totally depend upon risk acceptance criteria, keeping in mind the various risks involved in different strategy. The category where devices are bought from consumer market i.e. BYOD and OYOD, the OYOD will be very dangerous for use in the organization. In the same way HYOD will be very controlled environment, where employee will be least satisfied, so a balanced approach where enterprise level control exist on the device as well as there are options to have their own device according to their wish has to be considered. These two strategies would be CYOD and BYOD. An organization need to decide with their objectives by which strategy they want to go ahead [5].

Defenses and Measures

Defining the requirements for the secure mobile network:

a. ***Determining roles and responsibilities for managing and securing the device:*** There should be central administration of mobile device which would be assigning roles and responsibilities for managing and securing the device. The responsibility of the administration is to deployment of the devices, Add/Delete of devices, Connect a device, Device import, Edit device properties, Locate a device, Lock a device, Revoke a device, Selective wipe a device, Unlock a device and Wipe device and also define the policies, define the type of files i.e. public, private, protected and define users and end user policy [9].
b. ***Registry and inventory of mobile devices:*** All new mobile devices will go through a thorough procurement process registering details i.e. Model, Serial Number, Operating System, Device Id, Applications installed. Redistribution of the mobile devices – To secure the organization's data on a mobile device, the data is deleted by the admin when the user is no longer employee at organization. The device permanently deletes the data i.e. Deletion of only business data from the device that includes: Emails, Calendar entries, SMS, Memos, Contacts and Accounts, Browser cache, Accessed and Downloaded Files, Application and App data, Sensitive and Credential Information
c. ***Testing of applications to be installed on the devices:*** The applications will be installed onto the device after a proper testing procedure; the given testing's required i.e. Check for trusted certificates embedded in the application and its expiry, Threats to the application are identified, Vulnerability assessment is done, Calculate risk by risk metric framework and Determine if risks can be mitigated through the use of controls.
d. ***Efficiently installing and configuring security settings on the devices according to user profiles.***
e. ***Updating security settings, policies and patches:*** Update the patch release of application, configuration settings of the device and policies by pushing it onto the device from time to time according to the requirement and applicability, Anti-malwares are to be updated on a daily basis, Firmware updates of OS are to be pushed onto the device, whenever it arrives [11].
f. ***Training to employees on securing mobile devices:*** Train employees to secure business data on mobile device i.e. Presentation on risks to the device, Live demos on how device can be compromised, Lectures on importance of mobile security, Questionnaire on a yearly basis on mobile security. Manuals should be given, showing basic guidelines [11].

Control Objectives and Controls for BYOD

Controls: Controls are the safeguards or countermeasures to avoid, counteract or minimize the security risks over the organization assets and data [4].

Control Objectives: A **control objective** provides a specific target against which to evaluate the effectiveness of controls [2].

So, for the BYOD concepts Control Objectives are defined in Five Major parts which are given as follows:

a. Identification and access control
b. Data protection
c. Application security
d. Integrity control
e. Compliance

Table 1: Identification and access control

Identification and access control	
Enforce Strong Password *Objective:* To protect from the unauthorized access of the device.	
Restrict repeated characters	*Control* Restrict user from using sequential or repeated characters in their password
Minimum Password length	*Control* The password should be at least 9 characters long.
Require alphanumeric value	*Control* Passwords must have at least one letter or number.
Minimum special characters	*Control* Password must be having at least 1 non-alphanumeric characters (such as $, &, and!).
Minimum password age (in days)	*Control* The passwords shall be changed in every 60 days
Password history	*Control* Password history for a minimum of three previously used passwords should be maintained. New password won't be accepted if it matches previously used passwords.
Auto lock (in minutes)	*Control* Device auto lock should be set to 3 minutes. If the device isn't used for the specified period of time; it automatically locks in 3 minutes.
Grace Period for device lock	*Control* Grace Period for device lock should be 1min. i.e. how soon the devices can be unlocked again after use, without prompting again for the password. The time limit is maximum 1 minute. Setting this to immediately will require a password every time the device is unlocked.
Maximum failed password attempts	*Control* Number of maximum failed attempts is 10 and after the limit is crossed; all the data and settings are securely erased from the device.
Authentication *Objective*: To verify the user and the device.	
Two factor authentication	*Control* To prevent the device from unauthentic user or from the unwanted access on the device use two-factor authentication which includes the following– 1. User Name and Password for user authentication. 2. Digital Certificate- Exchange of trusted certificate between the mobile device and enterprise services to authenticate the device by using the Digital Signature algorithm
Network Segregation *Objective:* To segregate access to network of BYOD device.	
Guest Network for BYOD	*Control* The devices BYOD in nature can be connected to only guest network hence minimizing the risk of access to internal network.

Table 2: Data Protection

Data Protection	
Encrypt the data stored on the device *Objective:* To protect the data or resources related to the organization which is residing on mobile devices.	
Encrypt Data on device	*Control* 1. Internal Memory (Phone Memory): Use various encryption techniques like AES, DES, RSA or RC4 to protect the contact list, drafts, and Calendar, Memos and credentials information. 2. External Memory (Flash Memory): To protect the data stored in flash memory on the device use cryptographic keys which are generated by the system's Random Number Generator (RNG) using an algorithm.
Wipe data locally, remotely and selectively *Objective:* To protect the critical information when device is lost.	
Local Wipe	*Control* Initiate automatically local wipe of data after 10 failed attempts (all data and settings on the device will be erased).
Remote Wipe	*Control* Through MDM – As soon as any user reports missing or lost device MDM administrator should initiate remote wipe of the device.
Selective Wipe	*Control* The MDM can selectively wipe data on the device which can be certain sensitive documents, logs, configuration file according to organizations need stored in specific area.
Backup *Objective:* To maintain the availability of information when the lost device has been recovered or the device is formatted.	
Backup data regularly	*Control* Maintain backup of the device personally either using iTunes through cable or through iTunes Wi-Fi Sync.
Locate or lockout the device remotely *Objective:* To Locate or lockout the device remotely when the device is lost, stolen or misplaced.	
0Locate or lockout the device remotely	*Control* To locate/lockout the device remotely use an application from the application store of the device.

Table 3: Application Security

Application Security	
Certified business applications *Objective:* To avoid use of untrusted application.	
Third Party applications	*Control* Run business application which is duly signed by application developer's like- Code signing.
In-house applications	*Control* The in-house developed applications certified by the application managers of the organization.
Tested by security team	*Control* Tested by the security team of the organization and certified OK for use.
Management approval	*Control* Approval from the management for its deployment.
Download business application from controlled location *Objective:* To avoid download of malicious applications.	
	Control Applications are to be downloaded from

Organization`s application store	application store of organization where applications are tested and then placed on its server.
Blacklist and Whitelist applications *Objective:* To identify untrustworthy or malicious applications.	
Blacklisting	*Control* 1. Blacklist all applications by default and then provisioning of application done according to profiles and user groups. 2. The applications found to be malicious or untrustworthy are removed securely from the device and a blacklist is maintained so that it can never be installed on the device.
White listing	*Control* Maintain a list of application which is trustworthy on the centrally managed store such as MDM which will be given access through user groups.

Table 4: Integrity Control

Integrity Control	
Anti-malware application *Objective:* To protect device from malwares.	
Minimum functionality	*Control* It should provide runtime and static scanning on the device. It should protect, detect and remove latest viruses, worms, Trojan horses, spyware, Adware and most Root kit signatures on the device.
Tested and licensed	*Control* Run well-known, tested and licensed anti-malware application on all mobile/handheld devices
Password protected	*Control* Protect anti-malwares with password with reference to the password policy of the organization so that users cannot disable or uninstall the application.
Update	*Control* Keep anti-malwares updated with latest signatures.
Firewall application *Objective:* To filter inbound and outbound traffic.	
Minimum functionality	*Control* 1. Restrict on the basis of network traffic like Wi-Fi, 3G. 2. Restrict on the basis of applications. 3. Restrict on the basis of network traffic like Addresses, PIN and SMS.
Tested and licensed firewall	*Control* Run well-known, tested and licensed firewall application on all mobile/handheld devices as applicable
Rule set of firewall	*Control* Define rule set of firewall with reference to the requirements of profiles and user groups.
Establish VPN connection *Objective:* To maintain accuracy of data in transit.	
Minimum VPN settings	*Control* Use VPN controls and Digital Certificate for integrity control

Table 5: Compliance [17]

Compliance	
Risk management *Objective:* To incorporate mobile security into the company's overall risk management program.	
Including mobile security	*Control* Update the organization`s security policy by including mobile security into its overall risk management.
Maintain logs *Objective:* To monitor any unauthorized activities.	
Frequency of logs	*Control* The logs are to be maintained for every communication made between the device and organization`s resource.
Duration of Storage	*Control* Logs are to be maintained for at least one year.
Storage Location	*Control* The logs are to be stored at a centralized mobile device management server and at the VPN gateway.
Periodic audit *Objective:* To provide an assessment of system`s internal control.	
Security audit of devices	*Control* A periodic security audit of mobile devices is to be done; a minimum of twice in a year, to review the controls in place are working accordingly.
Compliance with international laws *Objective:* To comply with the law of the respective country with regard to mobile security.	
Compliance with respective country	*Control* Framework is to be modified according to the law of the respective country.
Privacy Issues of an employee *Objective:* To maintain the privacy of employee data.	
Segregate employee data from enterprise data on device.	*Control* Disk partitioning to be done, which would help selective wipe of data, if device is stolen or employee leaves the organization.

Managing BYOD:

So while talking about to manage the BYOD within the organization There are two models which can be used to manage the mobile devices in an organization to bring in BYOD.

a. ***Mobile Device Management:*** What is MDM (Mobile Device Management)?

The mobile device management tool helps the organization to fully control the devices which are generally supported by API`s of smartphones used these days. With the help of this tool organizations can lock down devices, enforce policies on the device, can encrypt the data or even wipe the data on the device locally or remotely. The MDM tool helps on the security and management of device by monitoring, controlling and protecting the device. It can do so by enforcing security settings, managing passwords, installing digital certificates for authentication. It can monitor applications installed on the device. It can even push for installation of applications on the device and enforce policies for the usage of that application. It can also even uninstall applications. It can generate reports and can manage the inventory of devices and applications. It can create groups for the devices and classify the files. Be it any platform of mobile device it acts as a single point for managing the devices. It also restricts user to download and install certain applications. It also helps to backup data and provides recovery services. In addition, the MDM is a tool that in a centralized manner controls the devices and can do over the air configuration remotely to those devices that are connected to the network.

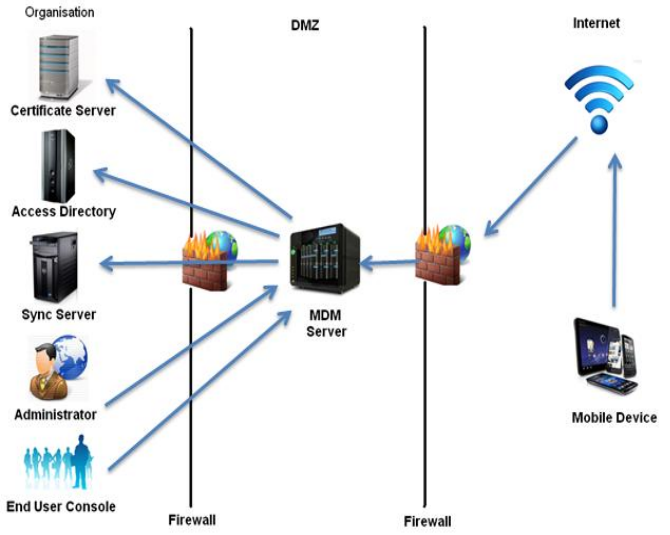

Figure 6: A MDM architecture.

The mobile devices are connected to the corporate network via an encrypted channel. The device platform can be Android, Apple, Symbian, and Blackberry. The MDM is placed at the DMZ which is public facing so that devices who are trying to communicate from external network can be enrolled and configured by the MDM. Also policies can be enforced and activity can be monitored, hence reports can be generated. The MDM authenticates devices by exchanging certificates from the organizations certificate server. With the help of Access Server, MDM can define access right. Also MDM can continuously sync and store backups of the data of organization to and from devices through the sync server. An administrator console which is inside the corporate network can manage the MDM by performing various tasks and request. Lastly, the user client side control on the devices such as changing passwords can be provided. All the communication is generally secured by SSL/TLS, to provide an encrypted channel.

The issues that MDM considers while managing the devices are as follows:

a) ***Device Management:*** The device manager manages the applications and software on the device. It is involved in the inventory of device. Management of various licenses is also done by it. MDM manages the configuration of the devices according to organizations policies. It remotely controls the device like locking and wiping. Also manages the session of devices to communicate with the corporate network.

b) ***Security Management:*** MDM considers various aspect of security like configuring the MDM itself, manages data security and applications. Finally it can also manage and integrate the various patches available.

c) ***File Synchronization:*** MDM continuously stores backup, manages the session to synchronize file transfer and manages various documents.

In a nutshell, MDM can act as a comprehensive solution for an organization to manage employee owned devices. Though along with it some added policies and controls have to be established for the appropriate security of corporate data.

Cloud Service:

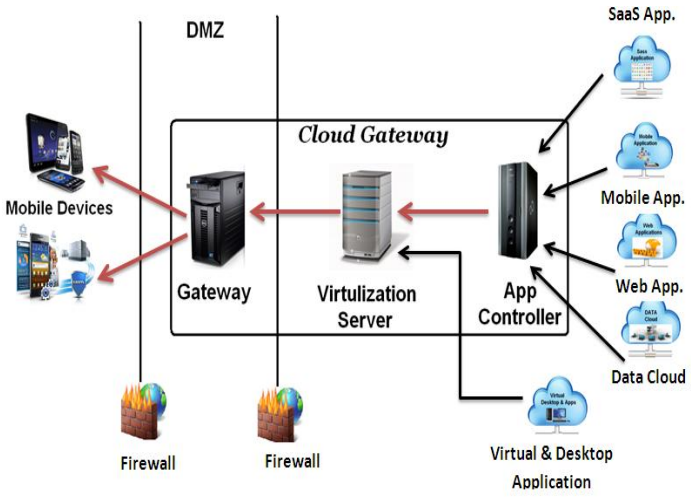

Figure 7: Cloud Architecture for Mobile Devices

According to the model, the client on the mobile device will access the service through an intermediary or broker which will be controlling the delivery to the end user. When a user/employee will try to access the data, he would undergo an authentication process which can be through certificates, tokens, smart cards or even SMS along with form based username/password mechanism which would ultimately be following a multi-factor authentication approach. Single sign-on functionality can also be integrated easily; the user on login will have an access to all the resources according to his/her privileges for that session. This session should be such that it can be used by the employee when they change their device to access resource. The session can be encrypted providing secure communication via SSL independent of the network (Wi-Fi or carrier network). The broker or the intermediary will manage the access of users to both data and applications in a controlled environment.

The broker here will perform the task of accepting or denying request of the users to access organization`s resources by basing its decision on seeing the users accessing, from where in the network they are accessing and finally the device used to access the resource. The client installed on the employees' device becomes aware of the device so that it can cope up with the heterogeneity of devices. Also the end users sessions should be device independent due to this reason. Also the broker will also enforce company policies. The broker hence would be a gateway to the organization`s resources which can be internal apps, external apps like mobile apps, data cloud, SaaS (Software as a Service) apps and data. Some apps would already be installed, and some can be installed or used on the basis of policies and access control mechanism through a authentication process. Hence the structure provides a security mechanism by which a sensitive data can be protected, as the data is on the cloud server and can only be accessed by authentic user with the addition of some controls like: Encrypting the traffic, Denying cut and paste transfers

between the virtual desktops and users client clipboard running locally and configuring policies so that users do have the ability to take print-outs and make a copy of their own [10].

FUTURE WORK

Future work will include:-

a. A proper R&D involving development of more appropriate model which can address security issues of organization and privacy issues of an employee in a BYOD environment.
b. More controls and control objective can be added.

CONCLUSION

As per the survey reports, more than a quarter of the survey responses i.e. 26% indicate that mobile devices of the employee are not permitted to access the resources of the organization and the rest of the data is all over the place. Apart from that survey indicates that 22% organization allow for employee to use own mobile devices which are managed by organization IT department and 21% almost matched by the percentage of organizations who are actually issued company-owned mobile devices, but expected to manage them on their own . There's clearly still a lot of confusion at this early stage about what should be acceptable or what should not be acceptable, and what different strategies to be required so BYOD should be managed [3].

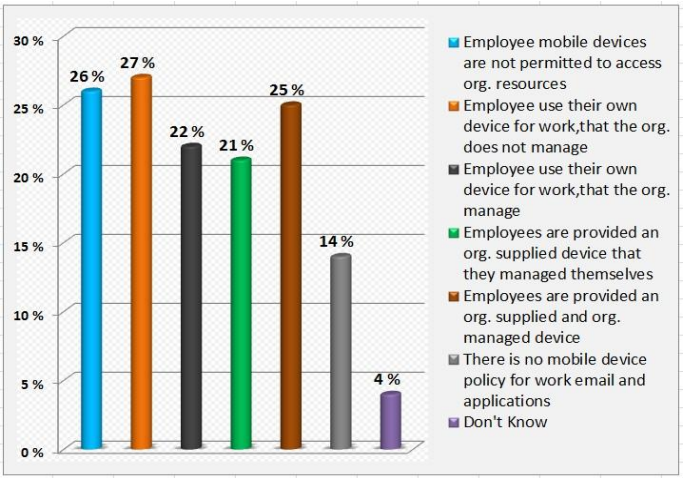

Figure 8: Organization's mobile device policy for work email and applications [3].

Protecting data on a device that isn't owned by the company is tricky. If the device isn't even managed by the company, it may be virtually impossible. More than half of those surveyed suggested it's either important or very important to be able to keep personal and business profiles separate, and segregate data on mobile devices [3].

a. Governance strategy for BYOD:

The governance of BYOD would start right from requirements of the organization which would attract the all the legal, statutory and compliance issues along with the policies of the organization itself to comply with it. For that the objectives of the organization must be clear according to how much they want to leverage their employees of using the device and data of organization on it in a restrictive manner or they want look forward and go ahead with Consumerization of IT (COIT) and develop mitigating strategies that come their way. For which the mode of operation would be decided to go ahead with. For implementation and management of data, device and people MDM and Cloud service can be used which would in turn give access to device, network and give location and time information. This would help in provided services to the employee such as Internet, data, apps, e-mails etc. according to user rights and need to know basis which is the requirement for the organization.

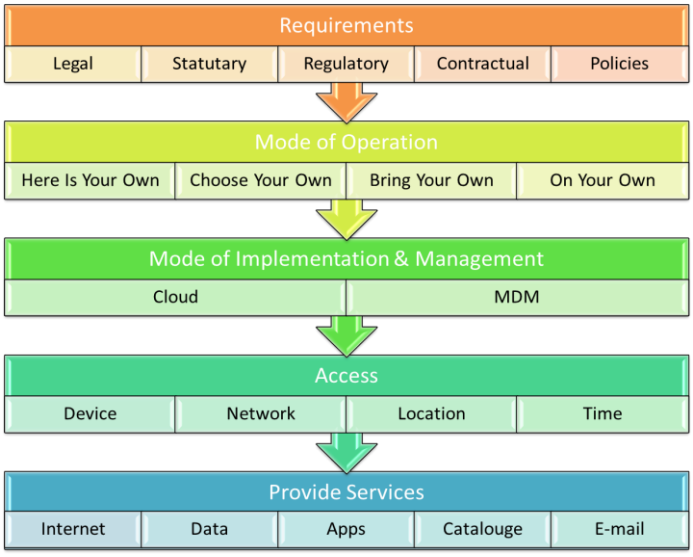

Figure 9: Delivery of IT service through BYOD.

REFERENCES

[1]. SISG Survey, http://esg-global.com/blogs/a-multitude-of-mobile-security-issues (as accessed on 1st February 2013)

[2]. http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5_Appendix_A.aspx (as accessed on 1st February 2013)

[3]. http://blogs.technet.com/b/security/archive/2012/08/02/byod-organizations-question-risk-vs-benefit.aspx (as accessed on 1st February 2013)

[4]. http://en.wikipedia.org/wiki/Security_controls (as accessed on 1st February 2013)

[5]. AarnoHarteveld blog, http://blogs.msdn.com/b/arnoha/archive/2012/04/25/building-a-byod-strategy.aspx (as accessed on 1st February 2013)

[6]. http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264 (as accessed on 1st February 2013)

[7]. http://en.wikipedia.org/wiki/Bring_your_own_device#cite_note-6 (as accessed on 1st February 2013)

[8]. "Forrsights Workforce Employee Survey, Q4 (Nov 2011)"www.forrester.com/Forrsights+Workforce+Employee

+Survey+Q4+2011/-/E-SUS887(as accessed on 1st February 2013)

[9]. Gordan Thomson (February 2012), ScienceDirect.com-Network Security-*BYOD: enabling the chaos*, Volume 2012, Issue 2, Pages 5–8.

[10]. Bill Morrow (December 2012), Science Direct.com-Network Security-BYOD security challenges: control and protect your most sensitive data, Volume 2012, Issue 12, Pages 5-8.

[11]. Steve Mansfied-Devine (April 2012), Science Direct.com-Computer fraud & Security-Interview: BYOD and the enterprise network, Volume 2012, Issue 4, Pages 14-17.

[12]. David Navetta, Bring Your Own Device Security and Privacy Legal Risks, from http://www.isaca-denver.org/Conferences/RMISC/Presentations/301-Legal_Implications_of_BYOD.pdf

[13]. Keith W. Miller, Jeffrey Voas, George F. Hurlburt (Oct 3, 2012), IEEE Xplore: Journals & Magazines - *BYOD: Security and Privacy Considerations*.

[14]. Bring your own device (BYOD) trends and audit considerations (Oct 2012), from http://www.sifma.org/uploadedfiles/societies/sifma_internal_auditors_society/bring%20your%20own%20device%20trends%20and%20audit%20considerations.pdf .

[15]. Kevin Johnson, Barbara L. Filkins (March 2012), SANS Mobility/BYOD Security Survey, from http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf.

[16]. Gerhard Eschelbeck, David Schwartzberg (June 2012), BYOD Risks and Rewards, How to keep employee smartphones, laptops and tablets secure.

[17]. Best Practices for Mobile Device Management, Maas360.com, from http://www.valleytalk.org/wp-content/uploads/2013/03/AST-0079353_mdm_bestPractices.pdf.

[18]. Miguel Angel Aranguren Romero, Haciendo Inteligente mi movilidad (Oct 2011), from http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/123.pdf.

