B.Y.O.D. Genie Is Out Of the Bottle – “Devil Or Angel”

Ms. Niharika Singh, pursuing M.Phil, University Of Pune, Pune

ABSTRACT
B.Y.O.D. (Bring Your Own Device) or according to some B.Y.O.T. (Bring your own technology) is a recent trend that has been observed where employees bring personally-owned mobile devices to their workplace to access company resources such as email, file servers, databases as well as their personal data. The concept of ‘Bring your Own Device’ is gaining momentum at the workplace. (Priya C Nair) Most of the companies in India and abroad have decided to apply this policy in their company by the end of 2012. Using personal devices at work is beneficial in some ways like more productivity, flexibility, freedom and choice etc. Besides it this policy has some risks as well like the prime issue of data security. It is found in the literature reviews that the organization who embraces BYOD policy found their employees happier, productive and collaborative. Hence the study was done with the primary objective of finding the views of respondents from different sectors and industries for the same. It also depicts the different threats that can be observed and also concludes whether application of this policy will be lucrative for the different type of organizations.

Keywords: BYOD, Personally owned mobile devices, UWYT, Productivity, collaborative, risks, threats, benefits.

INTRODUCTION
Bring your own device (BYOD) is a new trend. It’s a business policy adopted by management where they allow them to use their personally owned devices like smart phones, ipads, tabs etc at the work place to access mails, databases etc. According to Bernnat, Acker, bieber & Johnson “Work is no longer a place you go to, and then leave, but an ongoing activity.” This policy is also sometimes preferably used in form of different terms like Bring your own technology (BYOT) or Bring your own behavior (BYOB). The time is to opt for the “Reach Out” approach that means “reaches out to employees, allowing them to use their personal devices – even PC’s – to do their work.” (Bernnat, Acker, Bieber, & Johnson, 2010, p. Many a time it is discuss that what was the reason of implementation of this model. It was none other than the demand of employees in company. Mainly the tech savvy gen today are well leveraged with all the technologies like smart phones, tablets and internet etc. that has made them approachable to all the world 24*7. This availability and flexibility they demand in their work life also so that they can do their tasks anytime and anywhere and that too with their UWYT model has no security issue and maintains cost but it was not able to bring the sync between the work and life balance ie it does not allows flexibility at individual level. The implementation preferable tools. Keeping this in mind management had to apply this policy in their organisation. It has been found that organisations embracing this policy have more happy, productive and collaborative employees. The issue doesn’t get over here, actually BYOD is a matter of cyber security. Many research has been done by various organisations on different sectors and it is found that majority of sectors found it fruitful except IT sector where various security issues like litigation, viral infection, unauthenticated users, leakage of confidential data’s etc. pop up. According to CompTIA , a trade organisation of Information technology industry, said in a study that security considerations are the greatest risk involved with this policy. But despite of its threat Indian companies are embracing this policy soon and they also permit their employees to bring their mobiles and laptops at the workplace. Thus BYOD concept carries different parameters with it. On one side it is lucrative and on the other side it has few risks.

In fact BYOD is the new concept replacing the older one i.e. Use what you are told (UWYT). Its just opposite model in comparison to BYOD, where the organisation has a tight control over the devices to be used in the organisation. Although of BYOD policy just reacted in a opposite manner by positive responses of the employees. Thus there were social, business, financial and management reasons to move to BYOD from UWYT.
That is the reason why UWYT is called as the current and BYOD as the future state. But BYOD is not such a simple policy, it has with its many drawbacks and carries many issues as well. Although the implementation of BYOD diminishes the assets and hardware costs but more sum of money needs to be spent on security issues, because after using this policy the official data are more prone to theft on employee devices. Another reason of this policy being deployed by organization is its complexity. Sometimes the employees does not welcome such kind of changes in the policy. In that case an organization should use a liberal approach for its implementation. There is a proposed approach by Leo De Sousa Ist 725 as follows:

The UWYT approach also followed by Policy development like Contract negotiations, Remuneration Policy, Information Security Policy. Third comes Technology Researches Management (MDM), Virtual Applications, Network access control (NCS) step of Implementation based on Policy and Research and last but not the least importantly the role of BYOD also called as Contain/Embrace Strategy which is
now a days very popular amongst the MNC’s and most of the companies have decided to apply this by the end of 2012. But the implementation of this approach requires leadership and proper project management. According to Chris Corbet in his article BYOD : Industry Trends and Best Practices there are 10 steps that can be followed for the successful implementation of BYOD. They are:

I. Creating a comprehensive BYOD policy – It includes decisions regarding which devices to be used, security settings, Applications to be loaded, Passcode etc.
II. Measuring your mobile footprint -
III. Simplify user enrollment
IV. Configure policies over the air
V. Provide self service capabilities
VI. Protect personal information (PII)
VII. Isolate corporate data
VIII. Continuously monitor automated actions
IX. Manage data usage
X. Track the ROI of BYOD

The implementation of BYOD is not sufficient enough to start with it. The most important and complex part of it is its security issues. For getting the best results out of it we have to look into some security issues which has been depicted by Bernard and Ho in form of Security Architecture Framework ie SAF with eight layers (Bernard & Ho, 2007, p.10)

PROS AND CONS OF BYOD
In order to overcome all the Threats related to it following are the few steps that can be followed:

- Well it is found that most of the people assess to company’s network through wi-fi connection which is unencrypted hence according to Michael Buckna, Communications engineer, Voice-over-IP provider enterprise systems group “there is a way to it by distributing and managing Virtual Private Network (VPN) solutions for all the mobile devices.
- The second risk that comes to mind is the stolen devices, infact it’s the most difficult one to face. These situations can be handled by changing email, dropbox, passwords etc. Few terms like Remote wiping, Locking tools, Mobile device management (MDM) are the IT solutions for the same.
- Next threats are the antivirus and malware which are dangerous for the user and the system as well. To overcome and prevent these threats, the systems and devices should be equipped with anti viruses and anti malwares. The different phishing techniques, poisonous apps and virus spreading tactics should be identified and users should be regularly informed about the solutions to it.
- It is talked that BYOD reduces cost but there are examples when the organization has faced the requirement of up gradation , such as at Kraft Food, where they gave their employees ipads as app resultantly, the company needed upgradation because more employees were assessing it.
- According to Ted Schadler, Sr. Vice President of Forrester Research, “The total cost of BYOD is higher than not supporting BYOD.”
Benefits of BYOD:

- In a survey by iPass of 1,100 mobile workers it was found that “employees who use mobile devices for both work and personal issues put in 240 more hours per year than those who do not.”
- Reduces the cost incurred and ongoing end-user management i.e., the maintenance and upkeep of the devices and appliances are no more the responsibility of the organization. Hence, the organization don’t need to look after the hardware and software as this is now done by the employees themselves.
- It will be now easy for users to switch to the latest version in time being which is not possible for organization.
- Gives time to focus on strategic decisions then to spend time in operations.
- Acts as a competitive advantage over others.
- Attracts best pool of employees from the market and offers flexi timings.
- Reduces the training time thereby increasing the productivity and efficiency of the employees.
- Application of BYOD at workplace will attract top performing employees because it facilitates flexible work time and often work-on-the-go.

BYOD increases the engagement of the employees in the workplace and after hours.
- According to Christian Childs, Marketing director, Dell, “BYOD is a business decision more than an IT decision. By embracing BYOD, the organization gets benefits from having a more productive and collaborative end-user environment, the ability to retain and hire top talent, for end users, it gives him more flexibility.”

Christian Childs, Marketing director, Dell

LITERATURE REVIEW
BYOD policy is a way to achieve social enterprise in an organisation. In words of Savitz, Eric Karayi and Sumir, “The employees also prefer to use their own devices rather than mandated by the company to get their work done.” When it comes to BYOD another term that comes in mind is Consumerization of IT that has dramatically changed the work culture and environment as well. The gen Y worker, also called as “IWorker” are more tech savvy and thus their life style. Hence for the organisations are also shaking hands and moving towards making a collaborated and communicated and satisfied workforce. In an article ‘BYOD is now Part of the Barrier 1:1 Complete’ published in PR Newswire US that Barrier 1, the leader in Intelligent Threat Management had announced a BYOD application that will protect users regardless of where they get network either it’s a public Wi-Fi. This application will secure the access by inspecting for viruses or malwares and give a safe search user experience. The popularity of BYOD policy is evident from the data and research of Research and Markets organisation who did Market analysis and forecasts of BYOD and found that 65% of the MNC’s will adopt BYOD policy by the end of 2012. The top reasons for this implementation are cost reduction and staff motivation but besides that there are threats in IT departments as well. According to the survey done by them, key issues are security, fragmented software and a rise in support costs. According to the study the companies which have said to implement this policy are Accenture, AirWatch, Alcatel-Lucent, Apple, ARM, Asus, Atmel, Authentec, Barclays, Cisco, Citrix, Dropbox, Enterprid, Fiberlink, Good Technology, Google, HP, HTC, IBM, IKEA, Intel, Intuit, Juniper Networks, LG, Mformation, Microsoft, MobileIron, Motorola, Nokia, OK Labs, PwC, Red Bend, RIM, Samsung, SAP, Sony, SOTI, Sybase, Symanetc, Tango, Tapatier, T-Mobile, Verizon, VMware, Vodafone, Wavelink, Zenprise.

According to Golia Nathan BYOD has three most important benefits in field of financial and health care industries. Those benefits include cost savings, robust connection and flexibility. In a study by Yun Haejung, Kettinger William J, Lee Choong, it is found
that use of Office Home smartphones lead to increased work-to-life conflict and thus created job stress and users resistance to use OHS. Though productivity is gained and it also reduces workload. Thus it has also been suggested in the paper that the work home conflict can be reduced by the proper segmentation of work. Employees now a days want to work at the new and advanced applications. I words of Bernnat, Acker, Bieber & Johnson, “Employees expect to be able to use all the innovative new devices and tools at their disposal, both to do their jobs and to maintain their always-connected lifestyles while being able to work whenever and wherever they need to.” These were the needs of gen Y employees that lead to a shift from UWYT to BYOD. But it is not as easy to shift from former to later as it seems. In one of the article of Leif-Olof Wallin, he has mentioned about four conflicting goals that should be taken into consideration while shifting from UWYT to BYOD are: Social means to keep employees happy, Business i.e. keep processes running effectively, Financial to manage costs and Risk Management i.e. to stop bad things from happening. According to Silicon India, most of the Indian business enterprises are adopting BYOD in their organisation. In a consumerization study conducted by IDC in 2011, it is found that despite security and support issues BYOD trend continues. In a paper by Burt and Jeffrey, they have mentioned that increased adaptation of BYOD have changed the attitude of the employees towards corporate network safety of business enterprises. It says employees are progressively using personally owned mobile devices including smartphone and tablets as well to access business applications. In a post by Pankaj Gupta, Founder and CEO of Amtel, a global mobile device management and telecom expense management vendor, it is mentioned that despite various application and software there are few mistakes that has to be avoided for the proper functioning of BYOD. Firstly, The appliances which are used for official purpose should get rid off few softwares and applications that can be dreadful. Applications may include such components which can introduce viruses or may steal data. Hence need is to manage the applications for secured data. Therefore it is necessary to block few of the blacklisted apps that can cause hazards besides that MDM solutions are the best way to protect your mobiles from viruses and various risky applications. Secondly, The devices should be protected with well complex password and the users should be forced to change them frequently in a fixed duration. Thirdly, The company should keep an eye on the extent of usage of the devices by the employee in case where the organisation is offering stipend or compensation for some part of the expenses. Hence an enterprise should look for a management solution that means real time visibility of usage and also give alarm when the employee is about to cross the threshold limit. The BYOD trend is increasing and more of the clients are adopting but in a finding by Onforce’s Q3 Confidence Index, where they have taken the opinion of 500 IT professionals, it is found that requests for mobile device configuration set up at the businesses in the past six months has increased to 25 percent. And the noticeable part is this, that this 25% is the only 31% of the total number of persons who made request. In words of Gene Morris, General Manager at BrightStar Enterprise solutions Inc “As businesses implement BYOD, there are significant mobile security issues to keep in mind.” In one of the issues Cisco Systems Inc. tried to assess the attitudes, fears and hopes for tablets and mobiles in the workplace and it was found that 48% of the respondents who were from IT said that their companies will not authorize the employees to bring their devices. In one of the research by BT it was mentioned that over 80% of the IT managers think that the organisations which apply BYOD policy gives them an competitive advantage over others. Dunnet Richard in his research paper has encouraged employers to accept the trend and hence the need is to develop clear policies to communicate to the employees. According to the Gale Sarah fisher, the BYOD policy is a low-risk, high-benefit program. “The BYOD policy is the result of consumer preferences and not corporate initiative” said Rege Ojas. Till now it was found that BYOD is useful for IT sector only but in a paper Burger Katherine has mentioned that in the banking sector also BYOD
has created excellent opportunities though accompanied by few costs and risks.

OBJECTIVES OF THE STUDY
Following are the objectives of the study:
1. Awareness about the BYOD policy amongst educational professionals.
2. To study the different threatening factors and the degree to which they are risky for an organization.
3. To study the various factors or benefits of BYOD that can motivate organizations to implement this policy.
4. To find out to what degree is this policy lucrative to the organization.

RESEARCH METHODOLOGY
The sample for this study consisted of employees from different sectors like IT, Consultancy, educational institutes etc. A purposive sampling technique was used to select the samples. Out of total 136 samples all the responses have been received but since out of them only 88 respondents were aware about this policy hence the data of only 88 respondents have been taken into consideration for the data analysis and interpretation.

DATA COLLECTION
Primary and secondary data has been used for the study. Primary data was collected through the written questionnaire and mail questionnaires. The questionnaire was structured and disguised type. It includes the closed ended questions only.

MEASURES
AWARENESS ABOUT BYOD POLICY

<table>
<thead>
<tr>
<th>AWARENESS ABOUT BYOD</th>
<th>AWARE</th>
<th>88</th>
<th>64.71%</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOT AWARE</td>
<td>48</td>
<td>136</td>
<td>35.29%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>136</strong></td>
<td><strong>136</strong></td>
<td><strong>136</strong></td>
</tr>
</tbody>
</table>

As it is evident that only 64.71% of respondents were aware about the BYOD. Besides that the second part of data analysis are the various threats that has been observed by various organisations after the implementation of this policy. Though according to the secondary data the researcher has found five biggest threats that are the barriers in the way of BYOD’s world acceptance. Thus respondents views has been taken for the same to find amongst all which are the most risky factors.

**THREATS OF BYOD**

<table>
<thead>
<tr>
<th>THREATS</th>
<th>MAXIMUM RISK</th>
<th>%</th>
<th>MEDIUM RISK</th>
<th>%</th>
<th>MINIMUM RISK</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORPORATE IT SECURITY</td>
<td>40</td>
<td>45.45</td>
<td>4</td>
<td>4.55</td>
<td>8</td>
<td>9.09</td>
</tr>
<tr>
<td>INCREASED COSTS</td>
<td>16</td>
<td>18.18</td>
<td>24</td>
<td>27.27</td>
<td>16</td>
<td>18.18</td>
</tr>
<tr>
<td>POTENTIAL THREATS</td>
<td>12</td>
<td>13.64</td>
<td>16</td>
<td>18.18</td>
<td>24</td>
<td>27.27</td>
</tr>
<tr>
<td>COMPLEXITY OF SET UP</td>
<td>20</td>
<td>22.73</td>
<td>16</td>
<td>18.18</td>
<td>32</td>
<td>36.36</td>
</tr>
<tr>
<td>LACK OF CONTROL OVER DEVICES</td>
<td>0</td>
<td>0.00</td>
<td>28</td>
<td>31.82</td>
<td>8</td>
<td>9.09</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>88</strong></td>
<td><strong>88</strong></td>
<td><strong>88</strong></td>
<td><strong>88</strong></td>
<td><strong>88</strong></td>
<td><strong>88</strong></td>
</tr>
</tbody>
</table>
Hence it is evident from the data that the most risky factor that is the biggest threat amongst all is the Corporate IT security and all these factors can be arranged in the sequence, starting from the biggest threat, of their risk as follows:
1. Corporate IT Security
2. Lack of control over devices
3. Complexity of set up.

Similarly the third part of the data analysis discusses about the lucrative factors of BYOD those are: Improved efficiency and productivity, Higher job satisfaction, Enjoy Increased mobility and competitive advantage over others.

**IMPORTANCE OF BYOD**

<table>
<thead>
<tr>
<th>ADVANTAGES</th>
<th>MOST IMPORTANT</th>
<th>LESS IMPORTANT</th>
<th>LEAST IMPORTANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPROVED EFFICIENCY AND PRODUCTIVITY</td>
<td>36</td>
<td>40.9</td>
<td>40</td>
</tr>
<tr>
<td>HIGHER JOB SATISFACTION</td>
<td>12</td>
<td>13.6</td>
<td>24</td>
</tr>
<tr>
<td>ENJOY INCREASED MOBILITY</td>
<td>40</td>
<td>45.4</td>
<td>2</td>
</tr>
<tr>
<td>COMPETITIVE ADVANTAGE OVER OTHERS</td>
<td>8</td>
<td>9.09</td>
<td>16</td>
</tr>
<tr>
<td>TOTAL</td>
<td>88</td>
<td>88</td>
<td>88</td>
</tr>
</tbody>
</table>
Hence it is quite clear with the data that the respondents has mentioned that the biggest advantage of BYOD is enjoy increased mobility and as far as the least important factor is concerned the respondents views are quite strange. Hence the advantages of BYOD are mentioned below:

1. Enjoy increased mobility
2. Improved efficiency and productivity
3. Competitive advantage over others

And last comes the degree to which the respondents feel that this policy can be lucrative for their organisation either may it be educational institute or IT or consultancy etc.

<table>
<thead>
<tr>
<th>TO WHAT LEVEL YOU THINK IS APPLICATION OF BYOD IS LUCRATIVE FOR AN ORGANISATION</th>
<th>1 (FULLY AGREE)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (FULLY DISAGREE)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>40</td>
<td>28</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>TOTAL</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Chart:**
- **Series 1:**
  - 1 (FULLY AGREE)
  - 2
  - 3
  - 4
  - 5 (FULLY DISAGREE)
Hence it is clearly evident from the figures that about 45% of the respondents agree with the view that BYOD can be lucrative for the organization. And only 4% of the respondents fully disagree with this view.

Thus it is clear with the data analysis that if BYOD has some threats & risks then on other way it is also accompanied by few advantages that have overshadowed its risks and that is the reason most of the respondents felt that it should be applied in the organisations but definitely with some security measures.

SUGGESTIONS AND CONCLUSIONS

In words of David Clarkson, HR manager at Cisco Canada, “Productivity happens where people are comfortable and using devices that are most comfortable for them.” Cisco was the first to apply BYOD in its organization. Similarly in a survey of 2000 people by VMware, a California based software company, it was found that 61% of employees feel more happier and more productive if they use technologies of their choice.

The corporate mobility landscape is growing complex as the employees use their devices like mobiles, tablets, smartphones which is a new trend also called as “Consumerization of IT”. Though various researches has been conducted on the same but taking the results of the Forrester consulting into account it has been found that the most important reason of deploying BYOD is increased workers productivity. The firms deploy different types of BYOD programs. They are:

1. BYOD programme for laptops
2. BYOD programme for smartphones
3. BYOD programme for tablets
4. BYOD programmes for home desktops/homes computers

“Worker productivity is definitely up. Employees are using devices that they choose and they can communicate with other workers more frequently.” (Government Operating Director)

“We are in the infancy of BYOD programs. These programs enable our company to get more return on employee time.” (Engineering consultancy, IT manager)

As far as the revenue and monetary benefits are concerned the study by Forrester consultant (2012) has revealed that the BYOD programme has the cost benefits also:
Besides this the data analysis which the researcher has done in the current paper also throws some light on the same. Results obtained from the survey revealed that the most important reason behind deploying BYOD policy is the workers productivity, though it is accompanied by many disadvantages but it has various advantages as well. The biggest threat observed is Corporate IT security followed by lack of control over devices and then complex set up. Hence the researcher suggest that though the policy is very lucrative will not only improve workers’ productivity but also helps in reducing costs increasing revenue. But the researcher suggests that the organization who are planning to implement BYOD should:

- Apply the security measures for the proper working of the devices and in order to avoid the damage or distribution of company data to unwanted hands.
- Train and Educate the workers so that should be prepared to use the applications that will be installed in their devices for security purpose.
- Although the maximum application of this policy is increase of workers performance and productivity but before using it the organization should find out the costs and benefits in order to justify the basis of application of this policy.

BIBLIOGRAPHY

[1] British communications (BT). Indian firms embraces BYOD. Lets_talkBT
[4] BYOD Adoption is growing amongst EMEA enterprises, despite security concerns; Survey shows(2012). Business Wire (English)
[22] Mulholland, Jessica (2012). Q&A: BYOD is better in Minneapolis. Government Technology July 17

[29] www.good.com/resources/Good_Data_BYOD_2011.pdf,