<table>
<thead>
<tr>
<th>S.NO</th>
<th>PARTICULARS</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>INTRODUCTION</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Meaning of Byod</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• History of Byod</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Byod Models</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Statistical data of Byod in different countries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Need of Byod</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Byod Drivers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Byod Risks or Challenges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Future of Byod</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Employee performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Updates of Byod</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Factors affecting Employee performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IT industry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implications of it leaders to overcome Byod barriers</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>REVIEW OF LITERATURE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bring Your Own Device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Employee Performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IT Industry</td>
<td></td>
</tr>
</tbody>
</table>
### RESEARCH METHODOLOGY

- Description of Research model
- Sample design
- Tools for Data analysis
  - a) Descriptive tools
  - b) Factor analysis
  - c) Reliability
  - d) Item to total Correlation

### RESULTS

FINDINGS

DISCUSSION

### CONCLUSION,

SUGGESTIONS

IMPLICATIONS AND
LIMITATIONS
INTRODUCTION

In present scene technology is dominating each and every walk of life. Now a days whole world is being tech savvy and mobile. They love to work with technology and want to be trendy at work. In k12 environments tablets, smart phones, laptops etc It becomes expensive for the companies to provide devices to employees for work.

Mobile devices or technologies which are being used by employees, students etc to work better and learn faster. Virtualization of work provides accessibility, flexibility, lowers computing and cost of production, improves
security and decreases carbon footprints. It helps to make employees global as they can be traced globally and can work from wherever they are.

**Bring Your Own Device** is a modern concept introduced in the corporate world to minimize cost of production, flexibility, improve employee performance. Earlier this utility was usually used in academic sector as they have already facilitated virtual local area networks. BYOD utility is must for knowledge workers in the present working environment. BYOD, BYOT, CYOT are really being very essential to meet current requirements and maintain performance standards of both individual and organization.

**Meaning of BYOD**

Due to lack of portability and several handling and assessing problems BYOD stands for the “Bring Your Own Device” this concept meant for the employees bring their own devices at their professional places for work. It’s a global phenomenon which is being used all over the world. It is usually used by IT professionals or IT leaders. It helps to blend employee’s personal and professional life together.
“Bring Your Own Device is a strategy that allows people to use their own devices, whether occasionally, primarily or exclusively for work.” (Citrix, 2012)

To date, BYOD has remained an informal practice for many organizations. It is observed that many employees used to bring their own devices for workplace, no matter whether this utility is part of organization policy or not. It helps to manage a huge data very easily.

In common words we can say that in simplifies the work of organization, lessens the cost burden of the employer, and strengthens employees at workplace as they can use applications, devices on which they can work more speedily and conveniently for better results. Use of personal devices at work is being common practice these days. Wikipedia defines:

“BYOD as a recent trend of employees bringing personally- owned mobile devices to their place of work and using those devices to access privileged company resources such as email, file servers and databases as well as their personal applications and data.” (Osterman, 2012)

Studies reported that 78% of U.S. white-collar employees use mobile devices for their work. 44% of knowledge workers telecommute once in a week. According to the report, improved employee productivity and job satisfaction are greatest benefits of BYOD. It also lays down some challenges in front of IT leaders. Employees wanted to control their work which was not possible in company owned devices COD. They also want to work with the device and applications of their own choice. Commonly, employees prefer to use desktop virtualization to make mobile their work. (Barbier, Bradley, Macaulay, Medcaif, & Reberger, 2012)
Now firms are adopting technologies to make office work paperless. Paperless office would eliminate the use of paper and its storage. Approximately 61% firms have adopted these technologies. Technologies helps to handle “Big Data” of firms related to Finance, Accounting, HR, marketing easily. According to the study 23% of firms already embraced or adopted mobile technologies. Document management system: it is a tool to make paperless office. It provides several benefits like reliable data security, effective sharing, document, retention. If allowed accessibility of it provides professional to save their time to work from anywhere in the world. It maintains the work flow in the organisation along with security of data. It makes firm more productive and time saving.

“We want our people to feel supported with the latest tools to do their job and knowledge connect demonstrates how committed we are to the attraction and retention of new talent. Knowledge connect gives us a competitive advantage and helps us compete with firms much larger in size.” (kluwer)

Devices are dictating the market today. Devices are being used by employees whether their employer facilitated BYOD utility or not. There are some differences observed in employee behaviour in different markets like mature markets, developing, high growth markets. BYOD is being driven by employee attitudes. Studies resulted that use of devices being useful in developing and high growth markets where employees are of thoughts i.e. “Live to work”. In this case they use to blur the line between personal and professional life. Work is being important for the people who work in these segments of market. They are not conscious about the work timing as well. (logicallis)

According to Richard Abelson; "Trying to stand in the path of consumerised mobility is likely to be a damaging and futile exercise. "Mark Quotes "BYOD
is about being innovative and helping your employees to work better" (Dean, 2013)

BYOD initiatives has evolved employee empowerment at workplace. Through BYOD employees feel motivated to use I phones and Google nexus at work. Employees were happier and comfortable to work with latest high speed technology. At the darker side BYOD can also be as a threat to business systems. Employees used this utility more for leisure than work.

BYOD is a reality of medium and small scaled enterprises. Consumerization of Information Technology was coined 2001 by researchers at CSC (Computer science corporation). This consumerization offers dramatically lower costs, luxury like big organisations, innovation, cost effectiveness.

HISTORY OF BYOD
The term BYOD was mentioned in a paper by Ballagas et al., at UBICOMP 2005. It first entered in 2009, courtesy of Intel when it recognized an increasing tendency among its employees to bring their own devices to work and connect them to the corporate network.

It took until early 2011 before the term achieved any real prominence when IT services provider Unisys and software vendors VMware and Citrix Systems started to share their perceptions of this emergent trend. BYOD has been characterized as a feature of the "consumer enterprise" in which enterprises blend with consumers. This is a role reversal in that businesses used to be the driving force behind consumer technology innovations and trends.

In 2012, the U.S.A Equal Employment Opportunity Commission adopted a BYOD policy, but many employees continued to use their government-issued BlackBerrys because of concerns about billing, and the lack of alternative
devices. In August 2014, a California court ruled that companies must now reimburse any work calls done on any employee's BYOD in the state (Labor Code section 2802).

To date, BYOD has remained an informal practice for many organizations. It is observed that many employees used to bring their own devices for workplace, no matter whether this utility is part of organization policy or not. It helps to manage a huge data very easily.

In common words we can say that in simplifies the work of organization, lessens the cost burden of the employer, and strengthens employees at workplace as they can use applications, devices on which they can work more speedily and conveniently for better results.

In a BYOD setting by Ovum, “the percentage of all employees using their own devices to access corporate data is up from 56.8% in 2013 to 69.2% in 2014”.

![Diagram showing BYOD, COPE, and Fleet Managed models](image)

Source: COPE or BYOD? Mobile Communication Device Ownership Options for Fleetswww.peoplenetonline.com (Blue, 2013)
BYOD MODELS

On the basis of sharing of acquisition of device and finance there are the different models of BYOD. Companies used to opt as per their requirement whether it is financial and infrastructure capacity of the company.

- **COBO** - Corporate Owned, Business Only. The growing trend of COBO or Corporate Owned, Business Only, promises to fix some of the concerns related to BYOD. The COBO model offers businesses a new way of acknowledging and embracing consumerization by giving some control back to IT without depriving users of the choice of devices that make them more productive. Only devices have mobile capacities can be used for business purposes. There is no choice of devices and technology to be used. *(Lalvani, 2014)*

- **CYOD, CID**: Choose Your Own Device, Corporate Issued Devices in this employer provide an opportunity or chance to employees to choose the device they like and feel comfortable to work in the organization. In this the liability of the device stays with the employer as he has to pay for the same.
• **BYOA, BYOT, BYOPC, BYOD**: Bring Your Own Application, Bring Your Own Technology, Bring Your Own personal computer, Bring Your Own Device: BYOPC it has usually been under certain circumstances, such as the employee being required to choose from an approved list of PCs, PC flexibility approach is likely to experience some growth The management tools available for differing PCs lack sophistication and despite various vendors providing tools that make managing PCs in much the same way as mobile devices are managed. The BYOD utility at work makes out-of-office and in-office collaboration a seamless process without impacting productivity. (James, 2014)

• **COPE, WSYD**: We sponsor Your Device In this everything is under the control of IT administrators and leaders of the organisation it is a kind of big brother situation in which employers fully manage and control devices. There is nothing like partnership ownership, control and liability of the devices lies in the hand of employer only. IT might offer multiple devices, apps and services from which to choose, but the available options might not be what users want or need specially when it comes to protecting sensitive data. In the end, it comes down to the same old battle that BYOD creates: management and security concerns versus flexibility and productivity.

**STATISTICAL DATA OF BYOD IN DIFFERENT COUNTRIES**

Statistics indicates that U.S. and India highly using desktop virtualization at workplace for mobility of the work. Following are the results of a survey on the basis of different regions of the world (Bradley, Loucks, Macaulay, Medcaif, & Buckalew, 2012)

**ASIA**
In **China** growth of mobile devices increased from 1.8 per knowledge worker to 2.7 from 2012-2014. 76% growth has been observed in the last two years who are expected to use BYOD utility.

In **India** it is observed that 30% companies support employee owned devices at their workplace. Highest percentage of employees is 69% in this country. Its usage increased per knowledge worker i.e. 2.8% in 2012 to 3.2% to 2014. India showed highest growth in the desktop virtualization strategy close to U.S. in the percentage of companies who are in process of implementing it.

**LATIN AMERICA**

**Brazil** will increase connected devices per knowledge worker 3.1% by 2014. In Brazil only 17% of IT leaders said that security is the major challenge while implementing at workplace. It indicated third highest percentage of companies who support BYOD utility i.e. 25%.

In **Mexico** 88% of IT leaders reported positively about this utility and its effects on employee performance at workplace. Here the growth per knowledge worker enhanced from 2.3 devices 2012 to 3.0 in 2014. Here in this country midsize firms had mobile policies to work with for better performance.

**EUROPE**

**United Kingdom** reported highest percentage of IT leaders i.e. 51% who believed in employee owned devices at workplace. Here IT leaders reported that lowering cost is top most benefit of this utility.

In **France** lowest percentage of employees who use employees owned devices at work. Highest percentage of companies who prohibits employee owned devices at workplace.

In **Germany** report indicated lowest use employee owned of smart phones, laptops, tablets. It is found during the study that 22% companies didn’t provide
any support for employee owned devices. Germany is the only nation where IT leaders reported and felt no benefit to BYOD is higher than any other.

In **Russia** IT leaders found that security issue as one of the top most challenge while implementing BYOD at work place. Here the study indicated the lowest level of desktop virtualization.

Survey results states that only 47% companies have a formal BYOD plan of Tablets / smart phones/ laptops at workplace which can be broken down in the following ratios on the basis of permission granted to all employees or some specific department or employees. (Rains, 2012)

**Gartner has stated that by the year 2014, 90% organizations will provide utility to their employees at workplace.**

**NEED OF BYOD**
As company issued devices used to be less user friendly so employees resist to work with these devices. Employee’s speed and productivity suffers due to this.

- **Market trend:** as there are many technology advancements can be seen in the market in every walk of life. So as in IT industry we can observe the entry of high tech devices.

- **Time saving:** BYOD utility saves the time of both employer and employee as employee can start working from anywhere anytime he wants and accessible to his employer 24*7 as required.
• **Standardisation:** It gives a sense of standard and status while working in the organization and using updated devices. It enhances feeling of loyalty among employees and help them to retain talented employees in the organization.

• **Technological up-gradation:** It indicates that the organisation is going with the trend in the market. Employees works faster, easily and in better way with the help of several new features of devices.

• **User friendly:** Employee may not be friendly with corporate owned devices and technology but they used to be friendly with the applications, technology and devices which they handle for their personal use.

• **Flexibility and accessibility:** BYOD utility has increased flexibility of work and employees can assess corporate data from anywhere in the world for corporate use. It blurs the geographical barriers between work and employees.

• **Employee empowerment:** BYOD utility makes employees self-sufficient at work. It works as a power tool for employees, they feel strengthen with these devices as they can work from anywhere and at any time.

• **Employee engagement**
Employee feels satisfied using this utility at work. It enhances the loyalty of employee towards the company.

• **Cost effectiveness**
Employer need not to invest huge capital in IT infrastructure of the company. They only share the expenses of maintenance and acquisition of employee devices.


BYOD DRIVERS

1. Improved employee satisfaction
As employee feels comfortable to work with the technology at their workplace introduction of BYOD program improves satisfaction among employees of the organization. Improved employee satisfaction (Networks, 2012), Employee morale can be improved (Osterman, 2012), Empower people (Citrix, 2012).

2. Increased employee productivity
Satisfied employees feel motivated and loyal towards the organization as a result of this they work better in the organization. Productivity, Increased productivity (Networks, 2012)

3. Greater mobility, flexibility and accessibility of employees
Technology enhanced the mobility and made employees more flexible work environment in the organization. Employees can start working from anywhere with the help of devices and can be traced easily.

4. Reduced IT costs
Use of employee owned devices has reduced the cost of employer to invest capital in IT infrastructure and It devices needed to make work simpler. It also reduced device management requirements for IT. Better quality of work can be expected if devices used by employees are their own as they use to feel very comfortable while handling their own devices their speed and quality of work
improves as a result of it. Reduction in cost, lowering communication costs (Networks, 2012), Lower support costs (Networks, 2012). Cut mobile cost by 22%. (White Paper, 2013)

5. Attracting and retaining high quality staff
Implementation of BYOD program in the organization opens up opportunities to attract fresh talent and retain quality staff to the organization. As talented employees like to work in liberal and free organizational environment.

6. Better care and longevity of devices
As the devices being used by the employees for work are their own they used to take proper care of devices and handle devices gently. They also keep updated their devices updated as per the trend and requirement of their designation and work. They care their own devices like their babies.

7. Faster on-boarding of employees and third parties
Everyone can easily assess the organizational web for clarifications of doubts and issues. The procedure of connecting to the organization is just a click away from the employees and customers.

8. Improved business continuity
As the process goes on without any geographical boundaries and interruption. Business continuity can be maintained through mail chains etc.

9. Blending of professional and personal work
There is a blend can be seen employees start working from their home with the help of devices. At the time of contingency or emergency employees can work from home with their devices. They can fulfil their personal, domestic and professional responsibilities together.

10. Organisation can keep up with the latest and greatest
Employees loves to work with technology and also want to work with highly upgraded and latest devices in the market. (Osterman, 2012), Other (Reddy, 2012)

11. **It is fueling mobile growth**
With the introduction of these BYOD kind of programs the purchase of smartphones, devices etc has been grown among employees as earlier they were not interested to do so for less domestic usage of devices. (Bradley, Loucks, Macaulay, Medcaif, & Buckalew, 2012)

12. **Simplify IT**
It has simplified the work of IT department they need not to invest a lot in acquisition of software and hardware for business purposes. Enablement of various multiuser applications has simplified the work of IT department along with enhancement of speed of work and save time and money together. (Citrix, 2012)
BYOD RISKS OR CHALLENGES

As everything is not totally fit or perfect similarly BYOD also possess some risk factors and limitations due to which companies may go through disasters. Some of those risk and challenges are here like :

As employee owned devices are more prone to data leakages and malwares. These data leakages and malwares may result into huge business losses to the companies.

• **Legal and regulatory problems, compliance requirements**
Legal protective rules for the information stored on devices. Business associates (BA), anyone with access to client information and provides support in treatment, payment or operations. Subcontractors, or business associates of business associates, must also be in compliance. PCI Data Security Standard (PCI DSS) has developed a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. GLB Act contains major components put into place to govern the collection, disclosure, and protection of consumers’ non-public personal information ; or personally identifiable information include: Financial Privacy Rule, Safeguards Rule , Pretexting Protection. (Osterman, 2012)(Reddy, 2012)

• **Content retention and management**
The data on the corporate network has to protect from leakages and malwares. Sometimes it becomes really very difficult for the IT professionals to save the content in case employee leaves the job. To solve this problem encryption is being used and removal of all details would be wipe off from the device of employees before leaving and can be locked its access.
• **Corporate Governance**
There are several policies and rules to manage and maintain records of the company. Government has also laid down so many legislations to protect the data of the company for maintenance of proper functioning of the company in the market. *(Osterman, 2012)*

• **Support**
Implementation of BYOD scheme in the organisation lays down a great challenge in front of IT leaders. As they are obliged to develop an IT infrastructure or network to fulfill and support all the requirements of the organisation and with compatibility to run on all kinds of devices. They have to monitor all the connected devices and also protect the corporate confidential and sensitive data from leakage. *(Reddy, 2012)*

• **BYOD costs**
As it seems that deployment of BYOD schemes in the organisation has reduced employers IT investment and cost of production. But it has increased the expenses and investment of employees. To handle the situation employers are obliged to reimbursing employees’ mobile expenses, processing related expense reports, investing in solutions to support heterogeneous devices and customizing apps to run on those platforms. *(Reddy, 2012)*

Inspite of above mentioned challenges studies reveals some more challenges like accommodate reduction in IT staff of the organisation, maintenance of highlevel of end user services and improved end user uptime. *(White Paper, 2013)*
**FUTURE OF BYOD**

Statistics Indicates that about 1/3 of organisations that do not currently have BYOD utility for tablet at workplaces. 19% companies plan to have BYOD utility for tablet plans and rest those who has not introduced smart phone BYOD plan yet i.e. 35% are planning to implement it.

Introduction of BYOD lays down several types of challenges through which organisation would have to go .similarly it provides tangible and intangible benefits to the organisation. The most important benefit of BYOD utility is to meet employee expectation at their workplace. It is a proactive approach of the organisation to increase productivity, mobility, flexibility in the organisation. It empowers employees at their workplace and makes them more loyal and futile. It creates a standard image in these K12 market environment and employees with the *millennial* mind-set.

If used with the right type of strategy BYOD can lead to

- Empower employees to improve their productivity.
- Security of corporate confidential data.
- Cost saving for the employer.
- Mobility in employees. *(Reddy, 2012)*

**COMPONENTS OF BYOD STRATEGIES**

In Mobile Iron employees are offered a choice to choose among options i.e. a corporate funded Blackberry a personally funded iOS, Android or other new generation device. *Monica Basso* predicted that by the year 2014, 90% of organisations will support corporate applications on personal devices. On the basis of customer experiences eight components of BYOD strategies are highlighted:

- Sustainability
- Liability
• Economics
• Device choice
• User experience and privacy
• Trust model
• App design and governance
• Internal marketing

**IMPLICATIONS OF IT LEADERS TO OVERCOME BYOD BARRIERS**

IT leaders of the companies used to face several problems while deploying BYOD utility in the organisation: like acquisition of different types of devices, protection of data and to develop a system compatible enough to work with different kinds of devices at a same point of time whichever operating system does a phone has like android 4.1, jelly bean, kitkat, windows phone, iOs etc.

Here are some strategies to resolve problems of IT department in companies like:

- **Infrastructure provisioning**
  Infrastructure of the organisation is designed in such a way so asto support all types of technical devices intelligently for the work. There must be technical ability in the infrastructure and manpower of the organisations to handle devices for work easily.

- **Virtualization**
  All the transactions and actions can be monitored and controlled from a centralized place of work which minimizes complexities and increases speed. It also helps to save the several resources of the organisation. It gives better controllability to the IT leaders of the organisation.

- **Containerization**
It helps to segregate data between corporate use and personal use through “container” structures it facilitates easy control of devices in the organisation. It also helps to divide secured application and data construct or a completely separate mobile OS via a hypervisor, organizations can isolate or contain corporate data on personal devices.

➢ **Encryption**

It provides a very strong protective cover to the BYOD programme to prevent it common and unauthorized access of the data along with malwares which can interrupt the functioning of the organisation.

**BYOD IN PHASES**

There must be some limits to which data and BYOD utility can be used. these limits helps in evaluating the requirements of employees for the work. IT departments have full control on these limits set by them while deploying BYOD programme for the reasons of security and number of devices allowed to be connected. *(Reddy, 2012)*

➢ **BYOD and Digital Divide**

It’s really a big question “Is BYOD bridging the gap or expanding the gap?” in the context of cost it has reduced the cost of production but on the other hand it has created a divide among low, middle and high income groups. Those employees who belong to low income group cannot afford smartphones, I phones, Tablets, Laptops etc. So there is a digital divide in the organisation as a result of usage of devices.

➢ **Smart Connect**

It provides identity – based access, device registration, and policy management for corporate and user owned devices of all types. *(Networks, 2012)* it is a kind of license to identity manager platform which solves the top most challenge of
BYOD i.e. security. Here IT leaders are responsible to assign a single user key at the time of new registration on the network.

➢ **Guest Connect**

This facility allows visitors and guests of organisation to use the corporate network without the threat of security. Through automation of this process IT leaders can manage the network easily. After registration and user identification guest can use this utility and it automatically connects to this device whenever it comes under this network. But the accessibility of guest connected devices used to be limited in nature. *(Networks, 2012)*

➢ **End Device Management**

There are several types of end devices being used by employees like laptops, I Pads, Smartphones, I phones etc. A simple network is not capable enough to run on or work with all types of devices being used by employees at work because of their different configuration and operating systems. For eg. There is a difference in compatibility of android 4.1, jelly bean, Kitkat, while using at work. Same difference we can observe in android phones, Iphones and windows phones. So to deal different types of devices at a same point of time. *(Networks, 2012)*
SECURITY OF BYOD

Security is a major challenge for IT leaders in the organisation. So IT leaders must employer and employee agreement having policies to protect the confidential and sensitive data from leakage and usage of data by unauthorized devices. Several measures used to be taken to maintain that are as follows:

➢ **Any device personal or business** (Citrix, 2012)
People or employees are free to choose there own device with which they are comfortable to work inclusive of windows, mac book, or laptops.

➢ **Desktop and application virtualization**
IT leaders can transform a single application with complete desktop through which data can be accessed from remote distances as per the demand of the users.

➢ **Self-service App store**
Staff can use any of the service applications or operating system according to their convenience and need of the work like windows, symbian saas etc..
Follow me Data
Employees can share the data inside and outside the organisation with the help of corporate network. IT can wipe of the history and data storage after transaction has been completed to protect it from leakage and unauthorised use of data.

Collaborative work platform
BYOD used to be collaborative platform to work as there are different applications of instant messaging and sharing information. There are several social networking sites through professional networks are staying connected personally and professionally. As they have to work with each other they must have the connectivity to all. It is also providing a global platform to work.

Easy online meetings
Online meetings became easy with the help of use of network on the devices. High definition videos have improved the quality of video conferencing. Public and private organisations can join meetings online and speak to each other through video conferencing.

Secure by Design (Citrix, 2012)
As data has been used on different devices so network must be strong enough to fulfill the data requirements of all types of devices. Above all a centralized data protection, compliance and control must be maintained to manage the data usage and applications which are being used by the device holders to a certain limit. BYOD environment must be like that works for both users and the enterprise for work purpose. There are Ten Steps to Secure BYOD like:

Determine which mobile devices are allowed on the network.
In the first step IT leaders must decide what devices have to be supported for the work in the organisation. It must be analysed before implementing this programme whether the device to be used fulfils requirements of our business or not. Employees must also be involved in designing access policy of BYOD in the organisation to understand the dos and don’ts of the policy.

➢ Determine which OS versions are allowed on the network,
After deciding the device to be used to allow on your network, you need to determine which operating system version needs to be installed on each device. Software packages and antiviruses must be kept updated so that the devices will not be susceptible for malwares. Mobile Device Management (MDM) software that users download and install on their mobile device automatically keeps devices up to date, much like the patching mechanisms used for updating desktop PCs.

➢ Determine which applications are mandatory (or prohibited) for each device,
Proceeding further the next step determine what applications employees need to be productive, and what precautions you need to take. An IT administrator can configure the MDM software to enable network access only to specified enterprise application(s), and disable access to personal applications that could carry a security risk while the user is logged in. When the user logs out of the company network, they can go back to using their personal apps. It helps IT leaders to protect sensitive and confidential data from leakage and keep devices under control of IT department.

➢ Determine which groups of employees will be allowed to use these device
This facility must not be allowed for all employees of the organisation at all levels. Only some specific segment, designations etc. must be there who are allowed to use organisations data on their own devices.
➢ Define the who, what, where and when of network access,
In this step association of users and groups with a specific network according to the policy you have defined in above mentioned steps. A unique identifier (such as a MAC address) to identify his device when it comes in the range of organisational data network.

➢ Educate your employees about the BYOD policy,
Employees must be educated to handle the devices at work in the organisation, about its policies, rules and legal compliances for the same. As almost all issues raised because of lack of awareness and lack of comfort during handling devices at work.

➢ Inventory authorized and unauthorized devices,
IT leaders must set up a control to enforce policies framed for the same they are required to conduct a reality check which and what type of devices are connected with the corporate data and who is using that. It provides visibility to the IT department and make sure that unauthorized devices are not connected.

➢ Inventory authorized and unauthorized users,
IT administrators also need to inventory all users (known and unknown) who are currently accessing your network.

➢ Control Access Based on the Need to Know,
It’s time to start enforcing the network access control policy—the Who, What, Where and When of network access control in the organization. IT administrators keep monitoring all the data, devices and users so as to prevent misuse of the devices at work.
BYOD is largely based on security risk and requirements of employees so IT leaders must keep update the technological needs of employees while working in the organisation like, apps, devices softwares etc.

DIFFERENT BYOD PROGRAMMES

Organisations used to deploy different types of BYOD programmes for different types of devices (Singh, 2012):

1) **BYOD Programmes for laptops, notebooks.**
Traditional laptop management systems were domain connected along with fragmentation and differences in administration for different laptop platforms. Bring your own laptop have also expanded the role of laptop management in the enterprise, changing how IT must manage these devices. Unified Laptop Management facilitates asset tracking, remote assistance, Software distribution, configuration management, User enablement end user self -service, secure content collaboration, Apps, Endpoint Protection.
2) **BYOD Programmes smartphones.**
In this BYOD culture smartphones are also allowed to use by employers for which they used to several sub programs to manage and control devices in the organisation. Mobile device management, mobile email management, mobile browsing management, mobile application management, mobile content management.

3) **BYOD Programmes tablets.**
Hybrid approach is implemented in the organisations which included corporate-owned devices and a BYOD program. as smartphones are being used in the organisation similarly tablets are also used.

4) **BYOD Programmes for home desktops.**
BYOD programme for desktop used to fulfill all the requirements of the organisation through a personal computer in the context of software, handling of employees and configuration. Shared Devices in Your Enterprise Mobility Deployment There are several essential activities takes place while implementing different BYOD programme for different devices like: Device choice, Device Check-in, Device Check-out, Manage and Secure Shared Devices, Configure Shared Devices, Privacy Concerns Security and Compliance. In the absence of these activities devices in the organisation cannot be managed and controlled properly for the organisational goal. As in different devices there are different kind of operating systems like blackberry, Symbian, windows, I Os, android etc. **(Airwatch).**
PRE-REQUISITES OF BYOD

It is not easy to assess BYOD utility at work place there are several preparations are needed for that before implementing and spreading this utility to the members of the company they must fulfil following requirements like.

➢ **Top management support**
Top management must prepare suitable policies for implementing this BYOD program to the organization with the advice of IT experts of the organisation.

➢ **Technical experts and Skilled manpower**
At the time of hiring this thing must be in the mind of the recruiter that the person he is going to recruit must be able to handle updated devices whether its computer laptop, I phones etc.

➢ **Trainers**
Those who are working in the organisation since these advanced technologies were introduced must be trained properly to make work easier and faster.
*Security and Compliance* (Citrix, 2012)

There must be multilayered security for the devices used by employees at the work place. There must be containerization and encryption of data to be used by the employees for the work. Data usage must be allowed in a certain limit as per the designation and nature of work of employees.

*Tech savvy manpower and customer*

As customers are tech friendly so employees at levels must be aware of the technology usage needed for the work or to communicate with the customer. It creates an environment of independency in the organisation.

*Network system*

Network must have the capability to allow the specified number of devices of employees of the organisation.

*Hardware requirements*

Organisations must possess basic requirements of the data like modem and personal computers, smartphones, laptops I pads etc.

*Eligibility* (Citrix, 2012)

Identification of persons who can use personal devices for work and personal use. Limit must be set for the personal usage of the corporate data along with certain distracting elements of data which may affect the work efficiency of employees. Employees must be allowed the facilities which are needed to do their work in nature as per their designation or profile.

*Allowed devices*

Only those devices must be allowed at work place who have the capacity to meet organisational work needs. No other devices must be entertained in the organisation. *(Citrix, 2012)*
➢ **Service availability**  
IT leaders shall be made available all the services, software, applications on BYOD devices and whether they differ by work groups, user types, devices and networks. *(Citrix, 2012)*

➢ **Roll out**  
Appropriate guidance must be provided to all the users and potential users while making choices among devices, applications etc. *(Citrix, 2012)*

➢ **Cost sharing**  
Employers must share the expenses occurred on the devices used for the professional purposes. They must also form some policies to bear reimburse the expenses and share the cost of acquiring and maintenance of the devices.

➢ **Device support and maintenance**  
Devices used for the professional purposes must be kept updated by the IT professionals of the organisation. They must keep updating employees about the useful applications, softwares, antiviruses, privacy settings etc. They must help them to solve hardware related problems of the devices. These in turn will lead to better results and security of the corporate data. *(Citrix, 2012)*

**REQUIREMENTS OF BYOD**

How to provision user owned wireless devices without jeopardizing the security of the network, How to limit access to network resources based on the class of user/device pair How to manage corporate-owned devices and user owned devices, How to scale without compromising the network bandwidth, How to keep track of devices and how they are being used,
How to manage a single user with multiple wireless devices (e.g. Tablet + smartphone). How to manage a consistent set of applications across a varying set of mobile devices. How to manage corporate data written to a mobile device. Can I assign specific bandwidth allocations to specific users or devices. Making BYOD administration easier for IT staff. (Networks, 2012)

LEGAL ASPECTS OF IT

As technology has simplified and speeded up the work of companies but along with these companies are obliged to face some legal risks obtained from deployment of this utility. As IT professionals has to protect their assets from their competitors and confidential information loss of this may harm company. BYOD utility is not fit for all types of companies and all employees in the company they must fix to whom they must allow to use this utility at work, data protection is also another which must be kept in mind while deploying this utility. Employee privacy is also an issue which must not be kept on stake with this utility as per employee’s Right to Privacy.

There are certain legislations are framed by the government for effective and controlled regulation of the IT devices and data.

Information technology law (or IT law). IT law consists of the law (statutes, regulations, and case law) which governs the digital dissemination of both (digitalized) information and software itself, and legal aspects of information technology more broadly. IT law covers mainly the digital information (including information security and electronic commerce) aspects and it has been described as "paper laws" for a "paperless environment". (Wikipedia)

Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction. Computer law" is a
third term which tends to relate to issues including both Internet law and the patent and copyright aspects of computer technology and software. (Wikipedia)

There are legislations like which maintains the implementation of IT in the corporate world like:

- **DATA protection act**
  Data protection is essential in case of outsourcing of work. It helps to maintain the trust and confidence of associated companies suppliers and customers. Here employers and employees are obliged to maintain trade secrets, corporate data, customer’s information, personal data etc.

- **Information technology act**
  Information technology act lays down provisions to protect confidential and sensitive data of the clients and customers. In this legislation 4 sections segregated into 13 chapters.

  Information Technology Act 2000 addressed the following issues: Legal recognition of electronic documents, Legal Recognition of digital signatures, Offenses and contraventions, Justice dispensation systems for cybercrimes, According to Section 10A of information technology Act,2000(amended in 2008)it also validates E-contracts.

- **Gramm-Leach-Bliley Act 1999**
  This legislation authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies. The GLBA permits sharing of personal information between companies joined together or affiliated as well as those companies unaffiliated. To protect privacy, the act requires a variety of agencies such as the SEC, FTC, etc. to establish "appropriate standards for the financial institutions subject to their
jurisdiction" to "insure security and confidentiality of customer records and information" and "protect against unauthorized access" to this information. (Wikipedia)

➢ **Electronic Communication Privacy Act**

The ECPA represents an effort by the United States Congress to modernize federal wiretap law. The ECPA amended Title III and included two new acts in response to developing computer technology and communication networks. Thus the ECPA in the domestic venue into three parts: 1) Wiretap Act, 2) Stored Communications Act, and 3) The Pen Register Act. (wikipedia, 2014)

All the legislative proceedings in a company related to violation of IT act used to be practiced by an **information technology attorney**. It is a professional who handles a variety of legal matters related to IT. The attorney gets involved in drafting, negotiating, and interpreting agreements in the areas of software licensing and maintenance, IT consulting, e-commerce, web site hosting and development, and telecommunications agreements, as well as handling dispute resolution and assisting with the client's Internet domain name portfolio. An information technology attorney works with engineering, IT, and other business units and ensures that customer information gathered by company is collected, stored and used in compliance with privacy policies and applicable laws.

Duties also include providing high quality, specialized and practical advice in business-to-business and business-to-consumer arrangements and advising on issues like IT outsourcing arrangements, software and hardware supply and implementation agreements. An information technology attorney contracts for web site developers and consultants in relation to on-line projects. Provides support and maintains confidentiality/know how agreements. Contracts for Internet service providers and data protection advice. (wikipedia, IT act, 2015)
EMPLOYEE PERFORMANCE

Performance: - An activity (such as singing a song or acting in a play) that a person or group does to entertain an audience, or an act of doing a job, an activity, etc.

According to Business Dictionary employee performance means, “The job related activities expected of a worker and how well these activities are executed. Many business personnel directors assess the employee performance of each staff member on an annual or quarterly basis in order to help them identify suggested areas for improvement.” It is a continuous process of communication between a supervisor and an employee that occurs throughout the year, in support of accomplishing the strategic objectives of the organisation. In it communication process includes clarifying expectations, setting objectives, identifying goals, providing feedback and reviewing results.

FACTORS AFFECTING EMPLOYEE PERFORMANCE

Following are the factors which affects employee performance while working in the organisation:

• Ability of employees
• Standard of living
• Knowledge and skill levels of employees
• Feedback from employers
• Environment of workplace
• Motivation level of employees in the company.

According to Jan West: 5 Factors that affect employee’s productivity are
• **Attitude is Everything:**
Researches indicated that happy employees found to be more productive and vice-versa. Negative thoughts also affects the performance of employees negatively which may result in hostility, absenteeism, attrition etc. To make employees happy at workplace employers are obliged to provide them facilities to make their work easy and fast.

• **Boss is the Barrier:**
Performance and productivity of employees highly influenced by the immediate supervisor or boss. If a boss never fulfil his promises, never acknowledge performance or gives credit to his team members, always keep blaming them for the mistakes and finding their faults. Barry L. Brown, President of a Florida-based consulting group said “A poor supervisor is definitely the No. 1 factor that causes low productivity,”

• **Productivity in sickness and in health:**
Employee’s health is a big challenge for employers to maintain their productivity and performance at their workplace.

• **It’s the Tech tools, stupid:**
Organisations don’t update themselves technologically and always try to avoid the utilities of tech tools like PCs, smartphones, laptops etc along with other latest technical tools which help to work employees higher and faster.

• **Downsizing and outsourcing Morale**
Downsizing and outsourcing techniques are highly being used by employers with the motive of cost saving and reducing complexities of the business but besides these benefits implementation of these techniques has direct psychological impact on employee performance, productivity and behaviour.
Management of employee performance generally used to measure behaviors, actions, or processes without also measuring the results of employees’ work. Performance picture completes when there is a balance between organisational performance plans and the real performance of organisation and employees.

Managing employee performance:– The Cycle
This cycle involves following stages like:

Performance management is the systematic process of:

- **planning** work and setting expectations
- **continually monitoring** performance
- **developing** the capacity to perform
- **periodically** rating performance in a summary fashion
- **rewarding** good performance
**IT INDUSTRY**

The OECD definition of the IT industry forms the foundation for this study: “it is a compromise, limited to those industries which facilitate, by electronic means, the processing, transmission and display of information, and it excludes the industries which create the information, the so-called ‘content industries’”

1G refers to first generation of wireless telephone technology (mobile telecommunications.) It was launched in Japan by NTT (Nippon Telegraph and Telephone) in 1979. These are the analogue telecommunications standards that were introduced in the 1980s. It is that the radio signals used by 1G networks are analogue.

Mobile generations took ten years to move from analogue technology to digital i.e. from 1980s to 1991.

2G Second generation 2G cellular telecom networks were commercially launched on the GSM standard in Finland by Radiolinja (now part of Elisa Oyj) in 1991. 2G technologies can be divided into Time Division Multiple Access (TDMA) -based and Code Division Multiple Access (CDMA) -based standards depending on the type of multiplexing used. 2G networks are digital. These systems were significantly more efficient on the spectrum allowing for far greater mobile phone penetration levels; and 2G introduced data services for mobile, starting with SMS text messages.

3G third Generation, is the third generation of mobile telecommunications technology.[1] This is based on a set of standards used for mobile devices and mobile telecommunications use services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.[2] 3G finds application in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV.
4G it’s succeeding 3G and preceding 5G technology USB wireless modems, to smart phones, and to other mobile devices. Conceivable applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, 3D television, and cloud computing.

5G (5th generation mobile networks or 5th generation wireless systems) denotes the next major phase of mobile telecommunications standards beyond the current 4G/IMT-Advanced standards. 5G is also referred to as beyond 2020 mobile communications technologies. 5G does not describe any particular specification in any official document published by any telecommunication standardization body. (Wikipedia)

TECH SUPPORT FOR BYOD FROM CORPORATE WORLD

Most of the telecom companies are taking actions to support BYOD with different kind of innovations which can minimize the risk or threat of BYOD users and make their simple and safe.

➢ INFOSYS

Ovum research indicated that Infosys Flypp™ digital experience offers a top tier app store solution for enterprises. Flypp™ is regarded as a well-developed ecosystem of services, huge repository of apps (comparable to Google play and the app store) and monetization processes. It offers multiscreen content delivery and Infosys proven integration abilities as key differentiators of the product. Infosys has offered comprehensive and scalable platform for digital asset monetization and value chain engagement. It also enriched with the tools and curate applications like video, commerce and advertising. (Devanahalli, 2014)
➢ **BLACK BERRY**  
Movirtu, a provider of virtual solution with the help of which multiple numbers can be active on a single device which provides users facility to use personal number along with a business number on a single mobile device. *(Blackberry Acquires Movirtu to Improve Adoption of BYOD and COPE, 2014)*

➢ **LG**  
This company has introduced LG-GATE which is an Enterprise-Ready Mobile Platform for secure deployment of BYOD utilities in the corporate world. This platform is competent enough to meet the security and privacy needs of BYOD users in the companies. Along with this users can explore different kinds of professional and personal experience with that. Initially launched LG G2, Gate promises a private and business virtualization experience allowing users to run two operating systems on a single mobile device. *(Ankeny, 2013)*

➢ **SAMSUNG**  
Samsung offers mobility to users with several features which helps in the management of an enterprise along with data protection and secure connectivity from anywhere. VPN and ODE ensures secure connectivity to the corporate data along mobile device management solutions to maintain the mobility with effectiveness and safety. Virtual private networks technology connects the enterprises to the world, transmitting corporate information and data far beyond the company’s firewalls and provides secure and reliable connection in the private and public network both. On Device Encryption (ODE) which is a sophisticated security system for mobile to prevent devices in case of loss or theft. Samsung enterprise customised applications to meet specific needs of the companies which in turn saves time and money of employees.
APPLE

Apple has also made efforts to bridge the privacy issues and mixed results. Google acquired an offering Of Divide which creates a separate workspace and device for corporate data and personal data. The main issue is privacy as once device is placed in control of administration they can track device from anywhere and can block or restrict any of the features of the device.

UPDATES OF BYOD WORLD

Google Buys BYOD Developer -- Folds It into Android Team

For Divide Google has purchased a BYOD developer which divided a smartphone into two split personalities to ensure that work and personal usage remained absolutely separate from each other. There is a remote management program provided by the companies to their IT leaders. This service works on both i phone and androids. (Mansfield, 2014)

California cell-phone ruling poses big BYOD challenge

California's Second District Court of Appeal ruled that companies with employees in California must reimburse those employees for work-related voice calls on their personal cell phones. The workers used their personal cell phones to contact customers about their orders and delivery. In its finding, the three-judge panel cited California labor code and noted, "We hold that when employees must use their personal cell phone for work-related calls, Labor Code Section 2802 requires the employer to reimburse them. Whether the employees have cell phone plans with unlimited minutes or limited minutes, the reimbursement owed is a reasonable percentage of their cell phone bills employees might be entitled to reimbursement for Skype calls and data service usage, or even for business-related uses of personal tablets, smartphones or laptops. (Hamblen, 2014)
IBM opens up smartphone, tablet support for its workers

Matt Hamblen, IBM has embraced -- nearly -- the growing "bring your own device" trend of allowing employees to buy and use their own smartphones and tablets for work tasks, said IBM's CTO for mobility, Bill Bodin. IBM workers will have email, contacts and calendar access through IBM Lotus Traveller, Bodin said. In addition to installing agent software on each device, IBM will enhance security through the use of VPNs and by requiring passwords for access to systems. The company will also deploy endpoint management tools that will allow IT managers to wipe data off devices that are lost or stolen.

(Hamblen, computer world, 2011)

CYOD to rise amid 'death' of BYOD in 2014, forecasts IDC Ryan Huang | November 27, 2013

SINGAPORE--Expect to see the death of bring your own device (BYOD) as an enterprise mobility strategy next year, which will be instead be taken over by a new trend Choose Your Own Device (CYOD), according to IDC's Asia-Pacific Predictions for 2014. The analyst pointed out one of his clients in Singapore saw its network bandwidth double in the month after they launched a BYOD initiative because "people were basically watching YouTube videos all day long". CYOD helps IT deliver tangible biz benefits like the degree of standardized environments, allows for easier management and security planning for the IT department. Different job profiles would also be eligible for different devices, and some groups may not even qualify to get any company issued gear but instead be given limited access on their own equipment.

(www.zdnet.com, 2014)

Analyst says this is an opportunity for BYOD software providers: "All of which leads to the conclusion that the backup suppliers really are missing a trick. It is quite literally a huge unfulfilled market. If the backup software makers had BYOD backup functionality in their products they could deploy one of IT marketing's greatest weapons - fear. So, why they don't remains a mystery:" (www.computerweekly.com, 2014)

IT Not Keeping Up with BYOD Use by Employees Friday, April 4, 2014
The employees are figuring out ways to use their devices for work that IT doesn't know about and/or doesn't approve. Part of BYOD policies needs to be keeping up with employees and getting their feedback on how they use BYOD. "End users are typically more advanced in the BYOD and consumerization "journeys" than their IT teams, said Mike Schultz, general manager of Windows server and management for Microsoft. That's not just limited to devices -- employees will use cloud-based tools and applications to help them get their jobs done faster. "There is a huge discrepancy between what IT thinks is happening and what users will admit to doing," Schutz said:" (searchnetworking, 2014)

With BYOD smartphones on the rise, IT headaches will become migraine

There's little doubt that the bring-your-own-device (BYOD) trend with smartphones and tablets has rattled a lot of nerves for IT managers. The situation will only get more The situation will only get more nerve-wracking in 2014 because of the 30% annual growth through 2017 expected for smartphones purchased under a BYOD approach, and the further emergence of Windows Phone as a third platform behind Android and iOS.

Geo-fencing for security "could be an elegant and simple way to solve problems," Stofega said.Windows tablets will also benefit from the apps that are already commonplace in enterprises, such as Word, Excel, and PowerPoint,
Stofega said. Android devices will make up 111 million of the 175 million BYOD smart phones shipped in 2014. *(Hamblen, Computerworld, 2014)*

➤ **BlackBerry Acquires Movirtu to Improve Adoption of BYOD and COPE**

Movirtu offers facility to segregate the personal and professional data. Movirtu’s virtual SIM platform facilitates users to use both business and number on a single device along with separate billing of calls, messages as per the usage of users. *(Blackberry Acquires Movirtu to Improve Adoption of BYOD and COPE, 2014)*

➤ **Migrating from Windows XP to VDI, Linux or BYOD. Is it a Non-Starter?**

Pcs which runs on windows XP getting down gradually. Now organisations are trying to migrate from Windows XP to Windows & or 8. VDI Virtual Desktop Infrastructure uses centralised infrastructure administrators host and share platform while working in the organisation. Mostly users access their virtual desktops from different kind of devices like clients, desktops, tablets, smartphones etc. This also oblige administrators to incorporate BYOD utility in the organisation. *(Dwyer, 2015)*

➤ **Why Processor Choice Matters To BYOD**

BYOD program is not necessarily to support all of the devices or their operating system. The devices that best match customer needs, security concerns, business demands and available resources must be used at workplace. Intel and ARM Holdings are the two competitors in the mobile chipset market. Intel’s high-performing Core-series processors power the majority of laptops, Ultra books and notebooks, and its low-power Atom processors are gaining market share in tablets, smartphones and hybrid devices. Intel’s all processors are prepared keeping management in mind, allowing administrators to reach
below the operating system level for additional security and accessibility (Admin, 2013)

➢ BYOD skyrockets in popularity for 2013- Here are the stats to prove it

In the whole year 2013 we have heard the term BYOD so many times. So many smartphones and devices have entered in the field of BYOD in this duration. Statistics predicts that by the year 2018 most of the professionals will conduct their work on their own updated smart devices. (David, 2013)

➢ Oracle Taps into BYOD Market with mobile Security Suite

One of the most popular software company ORACLE introduced a mobile security suite which supports organisations to run sensitive applications and data on users chosen devices. Here encryption facility is there for data stored on device along with separation of personal and professional workspace. (Oracle Taps into BYOD Market with mobile Security Suite, 2014)

➢ LG Gate tech separates work and play on BYOD smartphones

This is an innovation of LG electronics to reduce the complication of byod users related to security and safety. Another launch has been made by LG Gate 2 which is also enriched with more innovative than LG- Gate. (Ricknas, 2013)

➢ Research: 74 percent using or adopting BYOD

BYOD has brought a revolutionary change in the corporate world. In May 2014, Tech Pro Research's report, Research: Interest high in wearable’s despite low adoption rates, indicated that while most respondents had some level of knowledge of wearable’s, only 11% of organizations were using, planning to use or budgeting for wearable’s. (Hammond, 2015)