BYOD: ISSUES AND CHALLENGES

Shayan Khan
RGNCLC, NLIU Bhopal

Dr. Astitwa Bhargava
Faculty, RGNCLC, NLIU Bhopal

Abstract—*With the advancement of technology and the growth of 3G/4G services in our Smartphone's have created a new beginning for communication and data processing in the business world. The phenomena arising from last few years in business environment is BYOD (Bring Your Own Device), which illustrated that the employees use their own personal devices while accessing the company's resources inside or outside the organizational environment leading to new opportunities but many risks being associated with it. In this study we have discussed about the evolution of BYOD and several threats which occur while using personal devices. Also the privacy and compliance issues are discussed, followed by the security measures and recommendations.*

Keywords— BYOD, RISKS, PRIVACY

I. INTRODUCTION- BRING YOUR OWN DEVICE

Enterprises around the world are working towards increasing the productivity, efficiency and flexibility of their employee. Many IT executives are expanding the pervasiveness of mobility initiatives throughout the organization but they face the challenge to support the significant increase in the number of mobile devices used by the workforce. The people employed in the organization most of the time try to access information not only from devices within the corporation, but also beyond the firewall with smart phones, tablets, home PCs, and laptops causing corporate risk management where the data must remain protected [1].

The use of personal device by replacing the corporate-owned devices and supplementing corporate endpoints cover the several forms of BYOD.

BYOD [2] solution helps in the following ways-

- Giving people the privilege to choose their own devices to improve productivity, collaboration and mobility
- The protection of sensitive information from loss and theft while privacy, compliance and risk management is addressed
- The management is simplified and reduction of cost occurs. A single one comprehensive solution to protect data which simplifies the IT work.

II. EVOLUTION OF BYOD

BYOD began to grow in 2003 but it was only in 2011 the growth was very noticeable. In respect to survey report given by Cisco in 2012 this is referred as global phenomenon. The survey was conducted in eight countries in three regions (Latin America, Asia, and Europe) including both enterprises (1,000 or more employees) and midsize companies (500-999 employees). Figure 1 clearly shows that 75% of users in countries with emerging high-growth economies such as Malaysia, Singapore, Brazil, India, and Russia use their own mobile devices at work, while 44% of workers in countries with developed economies such as the United States, United Kingdom, Sweden, Italy, and Japan use their own mobile devices at work.

In 2013 Deloitte defined BYOD when the employee uses their owned devices in order to get access to the organization information and network. The BYOD policy enable employees access the data when at workplace but also allow them to access enterprise data outside the enterprise environment. In 2017, it was noticed that the security risk occur in the organization when they make employees use their own devices and using a business strategy using secure and safe BYOD MDM solutions or even prefer the shadow IT system. They let their employees use personal gadgets at work but all the apps and devices (not owned by the corporation) are not supported by its main IT department. It is possible to minimize the risks of users accessing important information by using BYOD MDM solutions or choosing the good BYOD policy. In the Gartner report submitted in 2014 it predicted that by 2018, 70% of mobile users will conduct all their work on personal smart devices. (Figure 2)

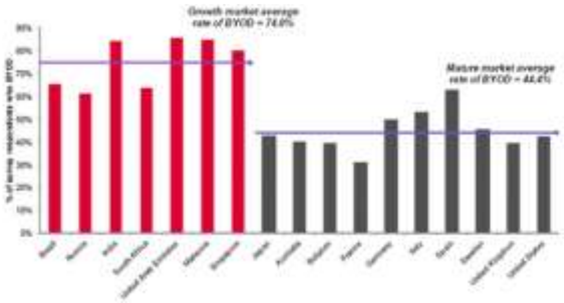
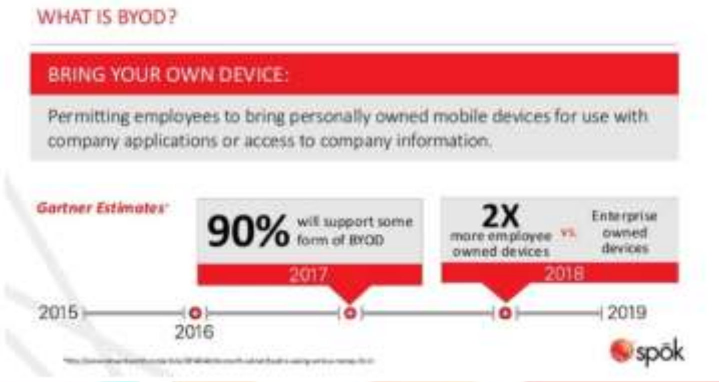


Figure 1- Level of BYOD deployment in both emerging economies and developed economies [3][1]

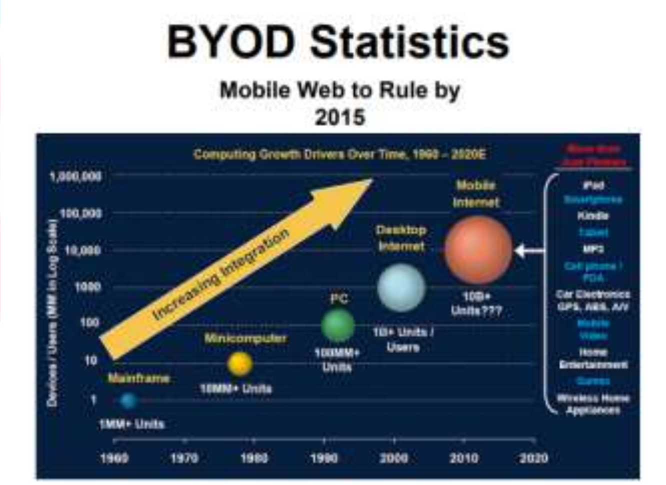

WHAT IS BYOD?

BRING YOUR OWN DEVICE:

Permitting employees to bring personally owned mobile devices for use with company applications or access to company information.

Gartner Estimates*
90% will support some form of BYOD
2017
2X more employee owned devices vs. Enterprise owned devices
2018
2015
2016
2019
spök

Figure 2- Trend of BYOD according to Gartner report [4][2]


BYOD Statistics

Mobile Web to Rule by 2015

Figure 3- BYOD growth over the years [5] [3].

III. THREATS AND RISKS DUE TO BYOD

- The confidential related to the company's work is many a times stored in the employee owned private devices and this can lead to loss of information causing a high amount of risk to the organization and client confidential data. Many a times it happens that once the access goes in the hands of an employee the enterprise has the lowest control over the data stored on employee device.

[1] http://journals.sagepub.com/doi/full/10.1177/2158244015580372
[2] https://iactivate.host/byod-2017-iphone-advantages-disadvantages-policies-and-practicies
[3] http://www.isaca-denver.org/Conferences/RMISC/Presentations/301-Legal_Implications_of_BYOD.pdf

- A DDoS attack performed by many compromised computing systems causing a coordinated attack on the availability of services of a target system or network. DDoS prevents regular employees from running machines on computer networks or their own personal devices will negatively impact on its server, and this will ultimately deny the availability of the system to legitimate users.
- Malware refers to malicious applications affecting both mobile devices and corporate applications. Mobile malware include applications with code embedded within them that compromise the security of a mobile device or related data. When a device is compromised by malware, corporate confidential data can be lost and corporate identities can be impersonated by the attacker. In addition, malicious applications can be encountered when a user visits a compromised site. More details on how malware affects BYOD.
- Vulnerabilities and Exploits. The organizational devices usually are better protected in terms of security and privacy standards and safe from any susceptible exploitation. While the individual employee devices most of the times do not comply to the rules, regulations and standards leading to a high count of vulnerabilities and when this vulnerable device is connected to a corporate network, they present new exploitable security holes concerning the whole network.
- Bluetooth and Wi-Fi connection also can infect a device, this happens when a mobile device is connected to a malicious network which can interpret all the data stored in it.
- One basic threat that is often not noted down is the users. The end user who is working on the sensitive information of the organization usually puts the data at threat, these people become a weak link in the company. Thus the focus on this end is also required. [6]

In an industrial report submitted, up to 60% of companies in the market face the issue of BYOD risks and the several other repercussions that arise from them. Confidential data like e-mail, documents, reports, files, applications, usernames and passwords, installed certificates, banking information, and web accounts can be accessible if a device is compromised or if it lost/stolen. The spam's which are received from known and unknown sources can lead to wastage of resources such as memory space and even bandwidth.[4]

IV. LEGAL CONSIDERATIONS RELATED TO BYOD

Protection to the employer is given under the IP laws, the Information Technology Act, 2000, where in the data of the owner and unauthorised downloading, copying, or extraction of data from a computer system or network by making the offender liable for damages.

In India still there are no specific case laws pertaining to BYOD issues, yet a district court in Texas in the case of RAJAEE VS DESIGN TECH HOMES, dealt with the question regarding the BYOD. The plaintiff, Rajaee, was an employee of Design Tech Homes, the defendant. The company configured the employee's personal phone and connected it to the company's server, allowing the employee to access company emails, contact manager, and calendar. A couple of days after the employee's resignation from the company, the company remotely reset the phone, wiping out not only all work-related data, but the employee's personal data as well. Aggrieved by this, the employee approached the court, seeking damages from the company. The case was dismissed on the grounds that the employee could not produce any evidence of losses incurred as a result of the actions of the company[5].

The various legal issues pertaining to BYOD are-

- Storage and Maintenance of Data
  The maintenance of integrity of data kept in the employee's personal device is very difficult to maintain. The data leakage also occurs through the unencrypted storage card kept in mobile phones. The main solution is accessing corporate networks by virtual private networks which creates a secure channel between source and destination and provides protection to all the data travelling over the network. This ensures the confidentiality of
  Of information in the network. Even by doing full disk encryption that data can be stored on secondary devices and secured therein.
- BYOD Security
  An approach of reasonable security must be adopted by the organizations implementing a BYOD strategy .A proper layout of security policies and technical controls are designed to uncover, detect and avoid any security risks. But in the conditions of the employees controlling over them is very difficult and thereby increasing the security and legal risks causing a serious issue in BYOD context.

- BYOD and Employee Privacy
  Employee privacy is another major issue of BYOD. The devices belonging to the employees contain lot of personal information such as photos, movies, account numbers, user names, and passwords, etc. and the same device will be used by

[4] http://ro.uow.edu.au/cgi/viewcontent.cgi?article=6446&context=eispapers
[5] https://ac.els-cdn.com/S1877050916000326/1-s2.0-S1877050916000326-main.pdf?_tid=f0c0d299-c923-4203-8a5b-b1d9d5a0bdd6&acdnat=1522039501_f0d34eb928aa44f0f2c901647a3742db

the organization which further have the power to monitor all the employee activities and can retrieve the information as well. If any data is needed to detect the security breach, the private or personal information of the device is also captured.

- Breach Response, Notification and Investigation
  The data handling in the organization is managed by the data loss prevention DLP software in which all the details are recorded in the log file. BYOD plans focus on those data also that has not been transferred to anywhere and yet accessible to public mistakenly even the personal devices are not possessed fully by the organization and when data breach occurs the organization will perform the notification procedure and risk assessment to identify the potential loss of data. Thus, proper BYOD strategies are to be developed and to be informed to the employees by the organization to overcome the foresaid issues in incident response and investigation.
- Secure destruction of corporate data
  The destruction of data is done by the company or when the employee is upgrading its own personal device. In both cases, the old device contents need to be removed in order to avoid the loss of important data. An unscrupulous employee can harm the company by passing on sensitive company data to public. One of the solutions is to remotely reset an employee's device by using Mobile Device Management tools. These tools are capable of deleting the partitions of data. Terms of employment must contain this clause so that when required, the complete reset of the device can be done without surprising him or her.

V. GOVERNANCE AND COMPLIANCE ISSUES

With the use of mobile device in the premises of an organization the compliance consistency often become a prime scenario to deal with and further BYOD introduces a complex environment when employees own the device and use it for personal data.

- PRIVACY GOVERNANCE
  The BYOD design given by an organization often interferes with the personal expectations of privacy of an employee. To overcome this main issue it has been addressed in the policies given by the organization including defined, clear expectations on privacy-impacting procedures. According to the regions, various organizations are forced to provide employees with a non BYOD alternative, potentially decreasing the savings potential of the overall BYOD program. For example, regulations in the US give organizations the right to monitor and wipe the users' device which acts as a critical step to assess the risks and even inform the users about the privacy implications of using their own device.
- DATA PROTECTION
  This protection of data in a BYOD deployment is not only concerned apply to corporate data. The regulation of EU governing the processing of personal data in a BYOD scenario will be applicable when the organization is collecting personal data from an employee's device and the purpose, expiration, security, etc., of the data collected must be clearly stated in the BYOD policy with the proper undertaking of risk assessment of the risks associated with the processing. The second scenario is the involvement of a a third party (i.e., if the organization utilizes a cloud email provider), it is important that the data be protected by a data processing agreement with the third party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.
- RIGHT TO BE FORGOTTEN AND ERASURE
  During the exit of an employee from the organization it is a common methodology adopted wherein the person's personal data erased, and for this the organizations adopt legislations which create a formalised approach on accessing the data and even the impact that will happen on the organization if the person knowing the company's sensitive information leaves the company.
- DATA OWNERSHIP AND RECOVERY
  The main dimension guiding the policy settings should be ownership which will create a system where all the personal and corporate devices will each have different sets of policies for security, privacy and app distribution. There should be a proper policy setup stating who owns what data, and whose responsibility it is to maintain backups of data, corporate as well as private and having a clear liability of loss, state whose responsibility it is to retain data recovery when it is needed, and the privacy implications of such recovery operations.
- MONITORING
  Several laws have been designed to illustrate the workplace monitoring, wiping and data protection according to the geographical background. According to the EU privacy regulations clearly states that the monitoring of the data should be restrained to use of the device within the time the employee is at work while the personal employee information is restricted by the Labour laws which vary by country.

VI. SECURITY FRAMEWORK FOR BYOD

A. Comprehensive BYOD Security Frameworks-The several measures adopted for BYOD security are as follows-

- Virtual Private Networks (VPNs), firewalls and email filtering [9][10], are one of the best resources for protecting network resources when the mobile devices are connected in BYOD without the enforcement of any policy. VPNs allow a controlled environment facilitating an exclusive network connection reducing the need for storing data and showing up a flexible work pattern. [11][12]. Firewalls help in protecting the network by monitoring and denying any malicious request while email filtering warns infected emails where in the mobile devices can sync email applications, therefore benefiting the device when email filtering is active.

- Network Access Control (NAC) helps in the permission management and denying the unrecognized device accessing the company's network. [13][14]. Identity and Access Management (IAM) helping in customizing the device access control and even managing the separation of duties while the access control installed on the mobile devices help in the identical access control functions. NAC also help in reducing the data leakage and malware infection attacks.
- Mobile Device Management (MDM) helps in controlling the mobile devices and its main component manages the protocols and provide monitoring and authentication of the mobile devices [15]. It facilitates in enforcing the access rights, conducting anti-malware scans, and providing activity reports which is useful in implementing the BYOD strategies and providing a [16] centralized, simplified solution.
- Mobile Application Management (MAM) is concerned with a specific set of applications on the mobile device which allows the company to apply security policies, lock down, define access control rules, configure software behaviours, remote wipe applications under its control, restrict access to unauthorised applications and install approved applications and also combined with containerisation.
- Desktop virtualization models enable the virtual machine and servers for hosting remotely located devices. Mobile devices operate like remote controls when interacting with applications contained on hosting hardware, and communicate via VPN connections. There are four types of end user virtualisation: virtual desktop streaming, application streaming, hosted virtual desktop & hosted virtual applications, which divide applications, operating systems and user profiles into independent, yet cohesive layers which adapt to user profiles. Desktop virtualisation models are low cost, centralise resources, data and security management and reduces or eliminates the need to transmit data onto mobile devices, thus reduces the possibility of data leakage occurring.

B. Single Purpose BYOD Security Solutions

- End user agreements, acceptable usage policies and liability agreements are formal contracts ensuring companies and employees mutually agree upon BYOD security policies; this is vital to the success of BYOD Agreements support all security controls in place, as they make certain employees know what is expected whilst using personal devices for work, and protects the business on legal accounts in the case of a security breach [1]. BYOD policies contain information such lists of permitted applications, installed security measures, management access, levels of access control, back up procedures, and rules concerning storage of data [2][17]. For example, employees may use VoIP applications, yet social websites are prohibited during work hours. Businesses are advised to involve employees when devising BYOD security policies in order to help them understand responsibilities [7].
- Containerization partitions mobile device storage space into independent sections in order to divide personal and work data. The section containing company data has its own security policies applied and allows remote access for company control, without affecting personal data [18]. The company can also specify a browser within the container to help secure online traffic. Gessner et al. suggests using containerisation as perimeter defence, where its internal applications utilise VPN connections to access resources in the company's network, whilst allowing policy management to direct control. Policy management includes rules controlling access rights of devices, and security procedures required to ensure the contents of the container are protected from threats which may be present elsewhere on the device [16].
- Remote wiping is the final reactive solution that is triggered when a device is lost, stolen or the owner separates from the company. The technique involves logging into, then removing all company applications and data residing on the device [15]. Some commercially available MDM and MAM solutions already contain remote wiping procedures

VII. RECOMMENDATIONS

- For a proper enhancement of security and privacy of BYOD the organizations should understand and properly execute their duties regularly and in a timely fixed manner.
- The BYOD policy designed should state the responsibility of employees regarding privacy and information security and should not affect the organizational ownership on BYOD devices and even the personal information by the BYOD users.
- The education of end user about the policies that guard the control of their mobile devices is very integral part. The policy should contain provisions signed between enterprise and employees under the End User Agreement (EUA) to create a common understanding about liability [17]
- Developing theory-based strategic options frameworks with suitable research methods (for instance design science) and focusing on the strategic actions by encouraging the empirical investigation of BYOD implementations using case studies, action research, and other qualitative methods.

- The other policies such as Here Is Your Own Device (HYOD) and Choose Your Own Device (CYOD) are also being used by several organizations [10] where HYOD includes the benefits of central control and even limitations of user adoption. CYOD policy is different in that employees select from a list of company approved devices to choose from. Giving employees a choice can increase chances of employees finding a device of their preference, encouraging adoption and limiting the number of devices supported by IT which would be cheaper than BYOD.
- Create a support and operation model using the scenarios formed by the mobility group, identifying and quantifying costs and benefits, will help build the overall business case for BYOD. Ensure that hidden costs such as increased data bills and support expansion are considered, together with potential advantages such as increased recruiting success rates with younger demographics.
- Test and verify the security of the implementation Perform security testing and review of the implemented solution. Assessments should be performed using an integrated testing approach combining automated tools and manual penetration testing, and preferably utilizing a trusted third party that has a proven track record assessing mobile deployments. We would recommend assessing the implementation as a whole and test devices, apps and the management solution together. In addition, it is important to test the infrastructural changes that are performed to allow mobile devices to connect to the enterprise network, such as Wi-Fi deployments or VPN endpoints.

VIII. CONCLUSION

BYOD is becoming more frequent in organisations over recent years. Innovations in mobile technologies in the consumer space have led to a change in user behaviour with IT Consumerization influencing employees to use their personal devices for work. BYOD has brought benefits to many organisations and new challenges over existing security, technology and policy to address in mobile enterprise strategies, some of which have been explored in this paper. From the examples reviewed in this paper it is evident that BYOD will continue to be a disruption for organisations to implement whilst protecting their internal data. The most effective solution for BYOD requires combining security, technology and policy into a comprehensive framework and striking the right balance between the three. Adopting strengths from the three would provide effective data security and compliance, policy that balances the needs of the organisation with the rights of employees and technology that supports policy. In the future enterprise systems could harness information from the physical, socio and cyber space becoming more intelligent in identifying users, providing right access to organizational information, detecting and responding to threats both from outside and within the organisation**.**

IX. ACKNOWLEDGEMENT

We would like to acknowledge our entire team which was a part of this research work. Even we had the constant support of our university faculty members providing us with their knowledge and experience. Apart from this our families and colleagues also played a vital role in providing timely help.

X. REFERENCES

[1] E. B. Koh, J. Oh, and C. Im, "A study on security threats and dynamic access control technology for BYOD, Smart-work environment," in Proc. Int. MultiConf., vol. II, Hong Kong, Mar. 12–14, 2014.

[2] L. B. Lau, M. M. Singh, and A. Samsudin, "Trusted System modules for tackling APT via spear-phishing attack in BYOD environment," Undergradute Research Thesis, School of Computer Science, Universiti Sains Malaysia, 2015.

[3] http://journals.sagepub.com/doi/full/10.1177/2158244015580372

[4] https://iactivate.host/byod-2017-iphone-advantages-disadvantages-policies-and-practicies

[5] http://www.isaca-denver.org/Conferences/RMISC/Presentations/301-Legal_Implications_of_BYOD.pdf

[6]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.

[7] http://ro.uow.edu.au/cgi/viewcontent.cgi?article=6446&context=eispapers

[8]https://ac.els-cdn.com/S1877050916000326/1-s2.0-S1877050916000326-main.pdf?_tid=f0c0d299-c923-4203-8a5b b1d9d5a0bdd6&acdnat=1522039501_f0d34eb928aa44f0f2c901647a3742db

[9] Dell Inc (2015) Dell Offers Top Five Best practices for Overcoming BYOD and Mobile Security Challenges. Paper presented to ENP Newswire Publishing, UK. pp. 1-3.

[10] Rhodes J (2013) Building Security Around BYOD. Managing Mobility, Rough Notes. Vol. 156. pp. 104, 114.

[11] Disterer G and Kleiner C (2013) BYOD Bring Your Own Device. Procedia Technology Vol. 9, 43-53

[12] [39] Wang W, Wei J and Vangury K (2014) Bring Your Own Device Security Issues and Challenges. Paper presented to The 11th Annual IEEE CCNC- Mobile Device, Platform and Communication, USA. pp. 80-85

[13] Dongwan, K., Changmin, J., Taeeum, K., Hwankuk, K. (2015) A Study on Security framework for BYOD environment. Institute of Research Engineers and Doctors, USA. Pp. 89-92.

[14] Koh, E., Oh, J., Im, C. (2014) A study on security threats and dynamic access control technology for BYOD, Smart-work Environment

[15] Keunwoo, R., Woongryul, J., Dongho, W (2012) Security requirements of a Mobile Device Management System. International Journal of Security and its Applications. Vol. 6. pp. 1-6

[16] Scarfo A (2012) New Security perspectives around BYOD. 2012 Seventh International Conference on Broadband, Wireless computing, Communication and Applications. Vol. pp. 446- 451, IEEE Press

[17] Wang W, Wei J and Vangury K (2014) Bring Your Own Device Security Issues and Challenges. Paper presented to The 11th Annual IEEE CCNC- Mobile Device, Platform and Communication, USA. pp. 80-85

[18] Keunwoo, R., Woongryul, J., Dongho, W (2012) Security requirements of a Mobile Device Management System. International Journal of Security and its Applications. Vol. 6. pp. 1-6.