**Advantages and Disadvantages of a BYOD Model in an Organization and**

**Legal Issues that Businesses Need to Consider.**

Deepa Natarajan

Department of Information Technology, Bellevue University

CIS 515: IT Infrastructure

Professor James Krohn

May 30, 2021.

**Advantages and Disadvantages of a BYOD Model in an Organization and**

**Legal Issues that Businesses Need to Consider**

Bring your Own Device- BYOD is a policy which allows the employees of the organization to bring their own devices and use it for both personal and business purposes. With the increased use of smart-phones and tablets, the availability of anytime anywhere applications and the more flexibility of allowing employees to work remote from home or travel finally, the pandemic has made BYOD an attractive option for both the employee and the organization. This sometimes referred to as “IT consumerization” (Disterer &Kleiner,2013) though opened up opportunities in increased level of employee satisfaction, increased productivity and less spending on hardware; it also has its own disadvantages in accessing the sensitive and confidential data from an employee-owned device, technical issues and legal problems.

**Advantages of BYOD Policy**

According to the article “BYOD Bring Your Own Device” (2013), this policy has paved the way for “user-driven innovations”, because the non-technical person in the organization can evaluate and select these technologies while the private owners of the devices who are familiar with the devices take these technologies to the home and apply the user knowledge to work, showing a new innovation path. Additionally, it claims that 50 % of 18 to 31 years old believe that the technologies they use in private life is better than the professional ones. (As cited by Forrester). Forcepoint.com states that, a study has shown that BYOD policy has increased the productivity by 16 percent. Increased employee satisfaction because of the familiarity and speed of the device along with the flexible working hours makes the employer attractive and helps in lower turnover rate.

“The most important chance of BYOD is the comfort users enjoy in using only one single device …personal and

Anything: business use beyond telephone and e-mail,

Anywhere: mobile use with a portable device connected via WLAN Internet,

Anytime: use during working hours and private times. “(Disterer &Kleiner,2013).

**Disadvantages of BYOD**

Lack of distinction between the private and professional space can lead to security threats. It is assumed that the incautious behavior in using the private devices will be carried while handling the company data. Moreover, mobile devices are considered as a highest security threat in this policy because of the lack of firewall or anti-virus software and possible malware attacks in using the mobile applications. Any software installation and malfunction need technical support from the organization, possibly increasing the spending on support; which brings the topic of support in terms of scalability and capability. Along with that, the organization may have access to the personal files of the users bringing some identity and privacy issues for the users. On the other hand, the if the device is lost or stolen, then data leakage can happen outside of the company network posing great threat to the confidentiality, integrity and authenticity of the company data.

**Legal/Ethical Issues with BYOD**

Dhingra (2015), discusses six possible legal and security topics associated with this policy viz., Maintaining and storing data, BYOD security, Employee privacy, Breach response, Remote wiping/blocking and secure destruction of corporate data.

**Maintaining and Storing Data:** This is an integrity issue, when the data is transferred over the public network. This problem can be overcome by using virtualized private networks, so all the data can be transferred in a secured channel. While storing data complete disk encryption will provide a solution for the secondary devices.

**BYOD Security:** Organization have little control on the employees’ devices and they have to completely depend on the employee to install or configure the security settings. If the employee is unwilling or not following the recommendations it can provide a loophole for the hackers.

**BYOD and Employee Privacy:** Organization have all the rights to monitor employee’s devices, the privacy trade off should be explained clearly to the device owners.

**Remote Wiping and Blocking:** Wiping, bricking or blocking of a device could damage the device or could remove the personal data of the employee. The device owner should be made aware of all the consequences in the BYOD policy in consent form.

**Secure destruction of corporate data:** When the company or the employee wants to upgrade the configuration then a complete destruction of data is required. In either case the removal of data can be done remotely using Mobile Device Management Tools under the technical support of the organization, which can prevent the sensitive data being leaked to public.

**Breach Response, Notification and Investigation**: In case of security breach, it will be inconvenient for the device owner to not use their personal devices until the investigation is completed. A proper strategy should be implemented and employees should be made aware about the consequences of previous security breach incidents and their responsibility of following procedures after the incident happened.

**Conclusion**

BYOD is increasingly attractive for being flexible and for providing remote working options. It also comes with the loopholes on security concerns for both the organization and the device owner. To secure the data, the organization need to take necessary precautions like updating the security products, using VPN, encryption and be on the alert constantly. Likewise, the device owner needs to be aware of the consequences of using the personal device for professional purposes. Transparent policies, clear consent forms and the proper training can help this new innovation to be strategically a successful model. In spite of all measure’s vulnerabilities can exist and it is the responsibility of every device owner and the management to maintain the integrity of the business data.

**Reference**

Georg, D., & Carsten, K., (2013). BYOD Bring Your Own Device. *Procedia Technology, volume (*9), 43-53, <https://doi.org/10.1016/j.protcy.2013.12.005>

Madhavi Dhingra., (2016), Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science, Volume* (78), 179-184, <https://doi.org/10.1016/j.procs.2016.02.030>

Forcepoint (n.d.). What is Bring Your Own Device (BYOD)? *Forcepoint.com.* Retrieved May 30, 2021 from <https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod>