Bring your own device: advantages, disadvantages, alternatives

Law

ASSIGN BUSTER

Introduction

Bring your own device or BYOD means allowing the employees to bring their devices to workplace. It was seen that nowadays technology has become the integral part of humans life so using this trend new policy was introduced in which one can enjoy using personnel devices in the office. It nowadays one of the latest trend to carrying personnel devices. It increase’s the employees productivity and allow them access more and more information. It has been observed that byod has increases the creativity level and innovation of the employees. It increases convenience of employees for doing work. As every coin has two side it has also got pros and cons. It has disadvantages like data leakage, device loss and many more. As one always carry their devices together especially mobile with sensitive and valuable business data and information it enhances the chances of mobile stolen or lost. It increases the risk of security for company. It is matter of concern for company to protect the data, secrets and valuable business monopolies. Files downloaded on personnel byod devices sometime contain malware which might affect the business data. Hence it is good and bad both for the company. It is how the policy is being implemented with strong set of rules and regulations. Personally, I think it is good for company but there should be measures to prevent security breach.

Advantages of BYOD

When employees use their own devices, they feel much excited and cheerful to do work. Reason is because there are using the devices, they are liking not the one they are provided by the organisation. As they are satisfied with their devices, so they are going to work happily.

Employees use mobile devices for work as well as personal purpose put in more hours a year than those who do not. It helps in creating the work surrounding in positive way. So, they are going to work freely and happily. BYOD helps companies free their employees to carry their phones and computers in accordance with business policy, which allows them to use the device they want and are familiar with for work purposes. It helps to work together from anywhere and anytime. It increases employees' level of creativity and innovation. Morale is another advantage.

Workers like to use the gadgets they are familiar with. The touch pad operates as it should, and where it should be, the power key is right. It allows employees to work comfortably as they access data from anywhere. It makes working style simple. They do not see it as extra workload when they work with their own device after work hours (Kevser Gülnur Gökçe, 2019). BYOD also increases the working hour of an employee as they can work from anywhere they want. As employees always complains about the gadgets they are provided with. BYOD reduces these types of complain and allow employees to work comfortably. BYOD also reduces the capital cost of organisation as they don't have to invest in gadgets. BYOD enables the organization to transfer computer hardware investment costs to its staff. Gives time to concentrate on strategic decisions and spend time in operations. As company now don't have to hassle about the maintenance of devices, they have just only look into. connection between employees' devices and organisation server. BYOD allows company to enjoy new technology and new interface, as it would be difficult for a company to invest more on gadgets and stay upgraded without having expenditure on the technology.

As we have seen in Michelin management it Attracts the best bunch of staff and provides flexible schedules. It will now be easy for users to upgrade from time to time to the newest version that cannot be done by company. IT department priorities: employees, especially not – so-tech-savvy, who work with company-owned computer gadgets will depend on your IT department for any minor issues they face. so BYOD will decrease the maintenance so it decreases the workload of IT department so that they can focus more on fixing the network and server.

Disadvantages of BYOD

BYOD execution isn’t enough to get started with it. Its security concerns are the most crucial and complicated part of it. As we have seen that the BYOD policy is good for the employees and organisation. Same there are some risks associated with it. There are no specific security features available in mobile so it is very easy to get into someone devices and fetch the important business data, personnel data. So BYOD increases chance of data leakage. If devices are connected to unsecured network than malware will get into the devices and spoils the business data, and personnel information which are very important information for company. As gadgets are very portable they are risk of getting stolen or theft along with the important data of company. Malware threat are nowadays big challenges to BYOD policy, it can be infected by malicious emails, marketing messages or via any social sites. Once it enters the device, they have every access to one’s devices. They can check the company email, can logged in to social apps, can have your private photos, can access the bank account or E-wallet and many more. Personal devices may not be sophisticated in terms of security such as anti-virus programs, patches, firmware updates and configuration settings (cindy zhiling tu, 2018). BYOD controls the users activities because it is used for both purpose personnel and organisational it would contain restrictive app which cannot be downloaded on the personnel devices, hence personnel freedom to operate the devices is affected. They are very conscious about their privacy as company can control their devices. Users privacy and freedom will be affected by BYOD policy. it makes employees lethargic because of mindset of working from anywhere anytime so they will not like 9 to 5 office. They use MDM (mobile device management) to control, supervise, manage BYOD devices. Sometimes employees don’t focus on the work while using their devices they involve themselves in playing games, enjoying social sites, chatting with the buddies. It distracts employees from doing their duties. many of them even don’t use the proper security for devices like password and forget about additional security like anti malware protection. As cloud computing have raised as trend, there is very concern of security regarding cloud computing. It increase’s responsibility for IT team. As SMEs doesn’t have enough fund so they don’t have enough IT professionals, to look after the IT department. BYOD’s total cost is higher than does not support BYOD. Thus, it is claimed that cost savings in the implementation of BYOD are only a fake face value; the expense of maintaining company information privacy is increased.

Suggestions for the right security practices to be introduced for a positive BYOD plan involve mentioning the devices that are authorized to be used, creating a strict security policy for all devices, placing out a clear service policy for any device that is listed under the BYOD criteria, explaining who owns what apps and data, choosing which apps are authorized and which ones are not authorized.

While deciding implementation of BYOD policy there are some factors taken care of. It should be taken care that policy neither be too lenient nor too strict if it will be too lenient than there will be huge risk to organisation, if it will be too strict than employees will use overshadow IT system and If it is too strict than employee’s freedom will be affected. Company should have enough operational fund to provide data allowance to every employee using personnel devices for company work. Allowing personnel devices also creates trend of using latest devices in office, as some can afford it but all cant because of their PayScale it creates insecurity between the colleague. Before implementing the BYOD policy every employee should be aware of responsibility involved. They should be aware of security threats involved in. Organisation should have proper IT team to look after security of data. there shouldn’t be any breaches in company’s network. It should have proper Application or firewall to monitor and manage security of devices. It should also be taken care of that employee’s privacy is been not affected. Company should invest on developing proper app to manage and monitor the system.

BYOD allow company to use new technology without investing on the Devices. Company also ensures employees are paid allowances on Time. They shouldn’t spend it from their pocket.

The BYOD experiences of Michelin North America and Rosendin Electric

The first reason was that management at Michelin was seeing BYOD as scope to increase productivity, flexibility of employees. while on other hand management at Rosendin Worries that BYOD will become a Headache for company. Management worries that employees would be too careless while using the apps, cloud, Technology. If we Want to implement any policy, first of all Management should have faith in the policy, but in the Rosendin case management were seeing this policy as Headache, rather than seeing as an opportunity. That’s was prime reason that policy didn’t work well in theirs case.

Management at Michelin found that BYOD increases the mobility of sales, customer support and operation whereas Rosendin management was confident about employees using the company-based devices which can be easily managed and monitored.

Rosendin uses MOBILEIRON mobile device management for its company based mobile and Tablets. If the device is stolen or theft mdm can wipe out the Data. MOBILEIRON allow to isolate business apps and data from personnel data and apps. Whereas in Michelin there is no such MDM for devices. It has collaborated with Cass information system it provides tracking and reporting of all ongoing devices. They can automatically register new employees, ensure policy acknowledgment. It increases the mobile enabled employees. It increases the job satisfaction and flexibility of employees.

Both the companies have one similarity that they are having the collaboration with cellular network. So, they Has choices in mobiles devices and cellular plan. so they can enjoy the newest technology. As they collaboration with the company they get discounts from all vendors. It decreases the cost of each devices. so they can also newest devices.

In Rosendin employees have to compulsory store the data in company authorized drop box they are not to allowed store in personal drop box If by chance they want to store the data in personal data. MOBILEIRON encrypts the data before storing in personal drop box.

BYOD at Michelin works well because the management was seeing the policy in positive manner, so they were doing their best to implement the policy in a good way. They were so serious about the policy that management of Michelin created a team from various departments like IT, human recourses, finance and legal department to develop and manage strategy for company owned devices and personnel devices. They have even tied up with cellular networks so the employees get good data plans and devices at discounted cost. initiative attracted mobile enabled employees. there sudden rise of employees. Company thought that it is good to implement BYOD policy with certain sets of rules and regulations.

Does BYOD Saves Company’s Money?

According to me yes it saves company’s money. All employee uses their personnel devices. So, the company doesn’t have to invest much on buying the devices, it cuts down huge capital cost of company. Company enjoys latest devices without spending much on the gadgets. It decreases the capital cost of the company; on other hand it increases the operational cost of the company. operational cost like data allowance, maintenance of MDM (which is going to manage and monitor the all personnel and company devices), other expenses. As there are more personnel devices it increases the operational cost of company because personnel devices are used both for company work and personnel entertainment purpose. It would be heavy burden for a company to maintain the heavy operational cycle.

Alternatives To BYOD

- COPE Corporate Financed / Personally Allowed: The company buys and owns the gadget, but it can be handled as their own by the staff member and used for personal matters. This provides additional control to the BYOD policy. It also creates a lot of personal privacy matters that may not be acceptable with many staff members. company will keep full possession of the mobile device and pay for its operational costs. Moreover, there are still ways for customizing the user who works with the device; they can still install non-work-related applications and adjust the software to meet their needs.
- CYOD Choose your own device: a whitelist of authorized gadgets is generated by the company, authorizing only BYOD for those devices. This can reduce privacy issues by permitting only equipment that you

know are safe. Sadly, if their gadgets do not qualify, this may leave workers purchasing new equipment. CYOD is often seen as a third option between the BYOD and other policies as it still allows workers a level of freedom to choose their phone. Sadly, employees might not be fully happy with the available device variety.

Conclusion

This assignment is about BYOD (bring your own device) which is nowadays the trend in workplace. In this assignment I have mentioned some of the pros and cons of BYOD. Company should take care of every requirement of employees and provide them a perfect a workplace environment so that they can work comfortably. BYOD is a good policy which fulfils the employees working needs. It increase's the employee's capability, flexibility and creativity. As there is proverb " Mind Your Man, they will mind the business". It means satisfy your employees; they will give the best efforts for the company. According to me BYOD shouldn't be taken as headache as taken by the ROSENDIN management it should be taken as scope to increase company's efficiency and productivity, as taken by Michelin management. Byod indirectly increase's the working hour of employees as they are not aware while doing the work at home, as it gives the feel of enjoying the personnel devices, Because there are some employees don't like to open company's device at home, so BYOD works in this case. BYOD is good for the company but it should be implemented with strong sets of rules and policies. Employees should be very well aware about responsibilities involved in carrying vital information in personnel devices. They should take a proper care of device to prevent it from theft or loss of devices. They should also follow the norms laid out by organisation. They shouldn’t try to overshadow the Company’s server like jailbreaking in IOS to install the restricted apps. According to me It is very beneficial for company, it is my view I can be wrong also, but personally BYOD is good initiative for a company. companies following the BYOD policy should be little conscious about the Policy.

References

1. Alex Koohang, M. T. R. P. H. N., 2017. SECURITY POLICIES AND DATA PROTECTION OF MOBILE DEVICES IN THE WORKPLACE. [Online] Available at: http://www. iacis. org/ [Accessed 7 November 2019].
2. cindy zhiling tu, J. a.,. y. z., 2018. Complying with BYOD Security Policies: A moderation model. [Online] Available at: https://aisel. aisnet. org/ [Accessed 30 october 2019].
3. Hollingsworth, L., 2018. Legal and Security Issues with Bring Your Own Device and Open Source Software. [Online] Available at: https://aisel. aisnet. org/ [Accessed 6 November 2019].
4. Kenan Degirmenci, J. S. M. H. B. F. N. P., 2019. Future of Flexible Work in the Digital Age: Bring your own devices challenges of privarcy protection. [Online] Available at: https://www. researchgate. net [Accessed 2 november 2019].
5. Kevser Gülnur Gökçe, O. D., 2019. “ Bring your own device” policies: Perspectives of both employees and organizations. [Online] Available at: www. kmel-journal. org [Accessed 1 November 2019].
6. Khalid Almarhabi, K. J. F. E. O. B., 2017. Survey on Access Control and Management issues in cloud and byod environment. [Online] Available at: http://d. researchbib. com [Accessed 2 November 2019].

7. Murat Topaloglu, D. K., 2017. Developing a BYOD Scale to Measure the Readiness Level: Validity and Reliability Analyses. [Online] Available at: http://www. jucs. org [Accessed 6 November 2019].
8. Otti, O. G., 2018. Bring Your Own Device (BYOD): Risks to Adopters and Users. [Online] Available at: https://repository. stcloudstate. edu [Accessed 2 November 2019].
9. S. flowerday, A. a., 2018. The BYOD information security challenges for CIOs. [Online] Available at: https://books. google. com. sg/ [Accessed 7 November 2019].
10. TRZISZKA, M., 2018. BYOD – A NEW TREND IN TELEWORK. [Online] Available at: http://cejsh. icm. edu. pl/ [Accessed 6 november 2019].