Bring your own device (byod)

Technology, Information Technology

Bring Your Own Device (BYOD) Assignment Bring Your Own Device (BYOD) is a relatively new concept in which employees are allowed to use their mobile devices to access the enterprise network. Although this is advantageous, it presents a number of challenges as well. The first major advantage is that BYOD helps to enhance productivity and overall employee satisfaction. Employees can easily respond to requests by clients at any given time, even when on the go (Egan, 2013). Through such flexible arrangements, employees generally tend to be satisfied with this work. Secondly, through the collaboration tools provided by these devices, employees can easily collaborate with one another thereby completing tasks faster and efficiently (Cisco, 2014). Third, BYOD is beneficial to the company since it lowers the cost of purchasing and maintaining the IT devices used for work. Fourth, when an organization adopts this strategy, it likely to attract and retain talented employees, especially the young. Finally, BYOD helps to transform the workplace by allowing employees use new and innovative ways to work. For instance, employees can take advantage of cloud computing and virtualization in doing their work.

There are a number of limitations associated with BYOD. First, BYOD implementation poses a major risk to the data held by an organization (Ernst & Young, 2013). Specifically, the use of personal devices to access company data may lead to leakage of confidential information. In order to address this challenge, many companies use virtualization where cooperate data and applications are accessed from a central position (Cisco, 2014). This gives the company control over its resources. In addition, containerization is also used where corporate data is put into separate structures which give the

organization enhanced control (Reddy, 2012). The second challenge is that the devices may provide an avenue for an enterprise network to be attacked. This may give unauthorized persons access to company network. In order to solve this problem, many companies are making use of encryption which makes it difficult for authorized persons to access company data. Encryption is also used to prevent users from accessing information from lost devices. Thirdly, BYOD may lead to many devices connecting to the company network since one employee may have multiple devices. This may reduce the efficiency of the network. To address this, companies manage the number of devices used on its network. This is mainly achieved through the use of passwords. Finally, when a company adopts BYOD strategy, it is likely that employees may take advantage and start to engage in personal or private activities instead to working (Ernst & Young, 2013). This may be addressed by asking employees to provide full report and feedback detailing usage reports of their devices.

In an article by Christian Buckley appearing in the TechRepublic (2014), the author gives real examples of how BYOD has been used. At one large non-profit organization, the IT society team realized that some groups were using the Dropbox without full authorization, and had been hacked. In this case, unauthorized persons were gaining access into company resources, and this compromised the security of the company data.

Based on the brief discussion, it is clear that implementing BYOD concepts in a real organization posses significant risks. In particular, BYOD exposes organizational data to a great risk, and this may prove costly to the organization. I would therefore not implement BYOD concepts in a real

organization since the costs associated with BYOD outweigh the benefits. Although BYOD might provide significant benefits both to employees and the organization, these benefits can easily be eroded in a single day or instance.

References

Reddy, A. S. (2012). Making BYOD Work for Your Organization. Cognizant Pp. 1-14.

Cisco (2014). Cisco Bring Your Own Device. Cisco Systems, Inc. Pp. 1-23.

Ernst & Young (2013). Bring your own device: Security and risk considerations for your mobile device program. Pp. 1-13.

Egan, B. (2013, October 4). BYOD As We Know It Is Dead. Forbes. Retrieved from http://www. forbes. com/sites/bobegan/2013/10/04/byod-as-we-know-it-is-dead/

Buckley, C. (2013, October 13). The Dark Side of BYOD. The TechRepublic. Retrieved from http://www. techrepublic. com/blog/tech-decision-maker/the-dark-side-of-byod/