Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2017, 4(4):163-165**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Bring Your Own Device

M. N.O. Sadiku[1], S. R. Nelatury[2], S.M. Musa[1]

[1]College of Engineering, Prairie View A&M University, Prairie View, TX 77446
[2]School of Engineering and Engineering Technology, Pennsylvania State University, Erie, PA 16563-1701

Abstract Bring your own device (BYOD) takes place when an employee carries a private smart device to an office and carries out business on it. This is the practice of allowing or encouraging the employees of a company to bring their own laptops, smart phones, tablets, camera, and USB drives and use them at work. This paper provides a brief introduction to BYOD and discusses some of its benefits and challenges.

Keywords bring your own device, bring your own technology, bring your own phone

Introduction

The proliferation of portable devices such as laptops, tablets and smart phones has led to a number of companies to allow their employees to bring their own devices to work.

Bring your own device (BYOD)—also called bring your own technology (BYOT), bring your own phone (BYOP) —refers to the policy of allowing employees to bring their personally owned devices to work [1]. This policy is often regarded as a subset of the consumerization of IT. It allows employees to have access to the corporate network, resources, and services including sensitive information through their personal devices as long as they comply with the company security guideline. It reflects a blurring of the line between personal and business use of the same device.

BYOD requires anywhere, anytime connectivity. Its pros include convenience for employees/students, easy to ask open-ended questions, relatively low commitment, potentially low cost. The cons include employees/students are using their own devices, they must have smart devices, and compatibility of various devices with different operating systems on the network [2].

Applications of BYOD

BYOD is widely adopted all over the world. Typical applications include cultural institutions, work places, business, healthcare, public libraries, and education.

BYOD has been adopted in educational institutions in US and UK. It allows students to bring their personally owned device to school for the purpose of learning. Students already owned these devices (including mobile phones, laptops, palmtops, tablets, and eReaders) with various apps and embedded features to use anywhere, anytime for the purpose of learning. Educators realize the power of technology in creating a learning environment that focuses on the "four C" of education: communication, creativity, critical thinking, and collaboration [3]. They employ smart devices thoughtfully to enhance students' reading, writing, speaking, listening, and language use. It is believed that the BYOD technology model will help young learners advance their knowledge [4].

Training and support are the main hindrances to participants implementing BYOD into teaching activities. Perceived advantages of BYOD include increased productivity, more effective time management, better

accessibility to data, and device portability for teaching activities [5]. BYOD initiatives in school can introduce challenges including network capacity limitations and equity issues for students who cannot afford their own devices. Some parents and educators question whether BYOD will cause distraction in the classroom and increase student vulnerability to cyberbullying. It has been observed that when students use the smart devices, they cause distractions including email, surfing the web, social media, instant messaging, and playing games. Students should be informed about the security threats of smart devices and their consequences.

Bring-your-own-device electronic examinations (BYOD e-exams) allow students to take an exam with their own laptop. BYOD e-exams are not actually secure, but they are better than the pen-and-paper examination [6].

BYOD has also been used to engage in interactive brainstorming and collaboration in order to inspire the next great invention. Employees may want to collaborate over Google Docs instead of using email company provided apps to share sensitive company data. Users have started to use their favorite apps (e.g., email, storage, or calendar apps) for work to collaborate [7].

Issues with BYOD

Opportunities using BYOD are found in the increased level of comfort of using one device anytime, anywhere. The comfort offered by BYOD leads to a higher level of user satisfaction and helps employees be more productive at work [8].

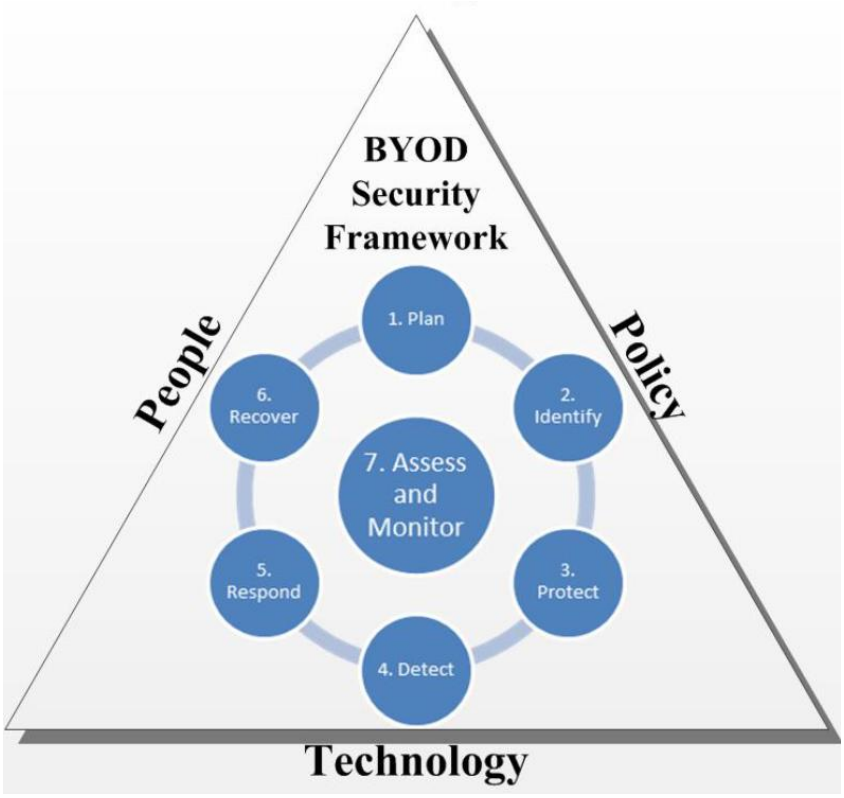

Figure 1: BYOD risk management [9]

The risk is seen in technical problems, in security, and in legal questions. BYOD brings significant risks such as leaks of company's confidential information. It has resulted in data breaches. A typical risk management is shown in Figure 1 [9].

Securing BYOD has some challenges due to the dual purposes of personal use and business use. Security tools such as firewalls and anti-virus software, which are widely used to protect corporate networks, can also be used to protect BYOD [10].

An employee using his own device may be susceptible from attacks originating from untethered browsing. Theft and loss are two major problems with mobile devices.

BYOD security concern can be addressed by having employees provide security requirements for each type of personal device that they use in the workplace. When implementing BYOD, employees should be given thorough training and required to comply with company-specific guidelines.

Conclusion

The use of smart devices at work has been around ever since people first brought their own USB flash drive. Initially, the idea of BYOD was not well received due to security reasons. But now more and more companies and educational institutions are supporting BYOD policies, creating a host of new challenges concerning security and intellectual property. The goals of BYOD are to increase the flexibility, convenience, and portability of personal devices in order to increase the productivity and morale of employees. BYOD is here to stay since its popularity seems unstoppable. However, the variation in laws among nations has caused great concern in the application of BYOD.

References

[1]. **"**Bring your own device**,"** *Wikipedia*, the free encyclopedia https://en.wikipedia.org/wiki/ Bring_your_own_device

[2]. J. Imazeki, "Bring-Your-Own-Device: Turning cell phones into forces for good," *The Journal of Economic Education*, vol. 45, no. 3, 2014, pp. 240-250.

[3]. I. Jones, "BYOD and Me: Teacher perceptions of a bring your own technology initiative," *Doctoral Dissertation*, Lesley University, March 2014.

[4]. Y. Song, "'Bring Your Own Device (BYOD)' for seamless science inquiry in a primary school," *Computers & Education*, vol. 74, 2014, pp. 50–60.

[5]. H. Berger and J. Symonds, "Adoption of bring your own device in HE & FE institutions," *Proceedings of the 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society*, July 2016.

[6]. P. Dawson, "Five ways to hack and cheat with bring-your-own-device electronic examinations," *British Journal of Educational Technology*, vol. 47, no. 4, 2016, pp. 592–600.

[7]. W. Widjaja and M. Sawamura, "Bring Your Own Device: Ubiquitous approach to digital affinity diagram collaboration," *UbiComp14 Adjunct*, September 2014, pp. 287-290.

[8]. G. Disterer and C. Kleiner, "BYOD Bring your own device," *Procedia Technology*, vol. 9, 2013, pp. 43 – 53.

[9]. N. Zahadat, "Mobile security: A systems engineering framework for implementing bring your own device (BYOD) security through the combination of policy management and technology," *Doctoral Dissertation*, George Washington University, January 2016, p. 26.

[10]. Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," *Proceedings of the 11th Annual IEEE CCNC- Mobile Device, Platform and Communication*, 2014, pp. 80-85.

About the authors

Matthew N.O. Sadiku (sadiku@iee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is an IEEE fellow. His research interests include computational electromagnetics and computer networks.

Sudarshan R. Nelatury (srn3@psu.edu) is an associate professor at Penn State University, The Behrend College, Erie, Pennsylvania. His teaching and research interests lie in electromagnetics and signal processing.

Sarhan M. Musa (smmusa@pvamu.edu) is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.