[*Dhingra *, Vol.5 (Iss.2: SE): February, 2018*] ISSN: 2454-1907
[*Communication, Integrated Networks & Signal Processing-CINSP 2018*] DOI: 10.5281/zenodo.1200272

IJETMR

International Journal of Engineering Technologies and Management Research
A Knowledge Repository

BYOD SECURITY AND ITS POSSIBLE SOLUTIONS

Madhavi Dhingra [*1]
[*1] Amity University, Madhya Pradesh, India

Abstract:
BYOD (Bring your own Device) is a piece of its bigger pattern consumerization, in which purchaser programming and equipment are being brought into the undertaking. BYOT (bring your own particular innovation) alludes to the utilization of customer gadgets and applications in the workplace. A powerful BYOD procedure can prompt various advantages for organizations, including enhanced representative employment fulfillment, expanded occupation proficiency and adaptability. BYOD can likewise give cost reserve funds from starting gadget buy to on-going use and IT helpdesk bolster as representatives put resources into their own gadgets. Despite worries about Bring Your Own Device (BYOD) security dangers, representatives over the previous years have appreciated the different advantages of BYOD. So too have businesses, who are far-fetched ever to prevent staff from conveying their own particular gadgets to work or utilizing them remotely for work purposes. The test stays to distinguish security dangers related with BYOD and locate the most fitting answers for alleviate these risks. By recognizing potential dangers, the framework can settle on an astute choice in the matter of how to react. This paper manages the security dangers related with it and the conceivable answers for it.

Keywords: *BYOD; BYOD Security; Device Security; Security Issues; Bring Your Own Device.*

Cite This Article: Madhavi Dhingra. (2018). "BYOD SECURITY AND ITS POSSIBLE SOLUTIONS." *International Journal of Engineering Technologies and Management Research,* 5(2:SE), 101-106. DOI: 10.5281/zenodo.1200272.

1. Introduction

As workforces turn out to be progressively versatile and accessible using cell phones, tablets and workstations, the venture turns out to be progressively in danger of information misfortune, regardless of whether by representatives losing gadgets or trading off cybersecurity.

The more effective BYOD executions are regularly those determined by business objectives (expanding workforce size or efficiency) rather than insignificant accommodation, and in that capacity, BYOD approaches ought to be worked through different divisions, for example, IT, HR, security and legitimate, to guarantee that the strategy stays adjusted on the undertaking's prosperity[1].

The program additionally needs to address the issues of workers, not simply IT staff's inclinations. Else, they may dodge the lumbering shields set up to secure the organization's

information keeping in mind the end goal to be more beneficial and streamline their own particular client encounter. Bring your own particular gadget (BYOD), as of late known as workforce versatility, is a standout amongst the most complex improvements for CEOs, since it acquaints gigantic dangers with information misfortune and information assurance.

2. Security Challenges

BYOD poses a number of security risks [2, 3, 4, and 5]. They include:

2.1. Builds Danger of Information Leakage

As our workforce turns out to be more dependent on cell phones, the conduits of information spillage and dangers open up, bringing about a considerably more noteworthy dependence on the IT division to secure cell phones. Cell phones and tablets are the weakest connection with regards to security and are inclined to assaults. They additionally require customary fix refreshes, with the obligation regarding these falling into the worker's hands. As per Gartner, by 2017, one out of two organizations will never again give gadgets to their representatives. In this way the onus is on the associations to execute approaches and systems that assistance representatives keep their gadgets secure.

2.2. Endeavors Vulnerabilities

CIOs are having less control over the cell phones utilized as a part of their association, which eventually implies they are more helpless against assaults. Representatives are downloading portable applications and associating with outside Wi-Fi spots without having the right security conventions set up. Truth be told, as indicated by an investigation led by HP, 97% of worker's gadgets contained security issues, and 75% needed sufficient information encryption. This makes genuine security openings that can be abused by programmers. This, combined with the way that your representatives won't not have against infection insurance or have an up and coming firewall exhibit on their cell phones, implies they are more defenseless against assaults.

2.3. Blending Individual and Business Information

A standout amongst the most evident BYOD security challenges is adapting to the capacity of corporate and individual information on a similar gadget. At last there will be sure kinds of information that will be uncovered all through the association, so thought should be given to the point of securing this information.

One of the greatest dangers to cell phones is malware that is introduced unwittingly by the client, which means malware could discover its direction onto the system.

The greatest hazard here that IT offices fear is the point at which worker's gadgets are lost or stolen. Over portion of security breaks happen when gadgets are stolen, so it's central that organizations are executing encryption strategies to guarantee that the gadget is secure against dangers. A straightforward however powerful approach to guarantee that representatives secure

their gadget is by inciting them to utilize even fundamental security highlights like utilizing a stick code.

Those representatives who don't stay up with the latest are at additionally danger of being focused by programmers. This incorporates portable working frameworks and in addition applications introduced on the gadget.

2.4. IT Foundation

BYOD expects CIOs to make adjustments to the present IT framework with the goal that it's BYOD agreeable. CIOs need to recognize which applications their workers are utilizing to connect with corporate information. Organizations need to guarantee that the information isn't just ensured, yet in addition adjusts to the present IT framework. Entrance testing ought to be done to recognize any vulnerabilities with the present IT home.

3. Security Measures or Solutions

Gadgets ought to have an equipment base of trust to ensure the association's touchy gadget, application and client private keys [6]. Ventures ought to have:

- A sound enlistment and provisioning process for worker possessed gadgets previously access to big business assets is permitted;
- A component for surveying the respectability of a gadget, particularly distinguishing if the gadget has been bargained at the stage level, (e.g., established, jailbroken) which would overcome the inherent security assurances that are given by the stage makers;
- A ability to seclude and shield the venture applications and information from whatever remains of the gadget condition;
- Enforcement of solid confirmation components utilizing the equipment base of trust before the client can get to big business applications and information from an individual gadget;
- Protection of the privacy and respectability of correspondences between the cell phone and undertaking administrations;
- The capacity to know who, when, what, where and how the endeavor information and administrations are gotten to; and
- The capacity to remotely wipe the secured condition for a lost gadget or possibly find the lost gadget.

Bring Your Own Device (or BYOD) arrangements are ending up increasingly prominent in the working environment, and it's not hard to perceive any reason why when you take a gander at the upsides and downsides. The greatest concern with regards to these new innovation remittances is security, and that is the place a solid BYOD security strategy becomes possibly the most important factor. The accompanying are a few answers for BYOD issues [7,8,9]:

3.1. Encryption

In any great rundown of vital hints to secure your organization's information, encryption is discovered, and that is the same when managing ensuring your business information in a BYOD situation. By encoding information as it is being exchanged to and from your workers' gadgets, and while it is on such gadgets, we can scramble it so it can't be perused without the correct passwords.

3.2. Applications for Remote Access

It's far better on the off chance that we can set up an easy to understand application that enables workers to safely get to our organization documents remotely, yet the application can be set to bolt out naturally after a specific measure of time of idleness. Whenever bolted, all organization documents are deleted from the gadget itself, however they are still put away securely in your organization's information servers, staying with your's information and your representatives' close to home information partitioned. The application, obviously, ought to likewise be scrambled.

3.3. Cell Phone Management

In looking at Bring Your Own Device security issues and challenges, you'll find that many list the fact that the business needs to control who can access the network, but they cannot control where mobile devices are going and what protocols are in place to ensure they aren't lost or stolen. There are solutions to this. Make sure there are protocols in place that will allow your IT department to manage a mobile device's (e.g. phone, laptop, tablet) access to your network. Mobile device management (MDM) is critical to make sure that a lost or stolen device cannot be used to access secure company information.

3.4. Identity Access Management

With any BYOD policy, you should implement some method of identity access management (IAM) to go along with it. You should specifically use one that uses two-factor identification to verify that an employee is the one trying to gain access to your business data, rather than a device that has fallen into the hands of someone who would compromise that data. To further prevent unauthorized access and the use of cached passwords, you should also have your company's BYOD IAM include frequent re-authorization, so your employees have to re-enter their passwords and won't stay logged into your company's data.

3.5. Set Specific, Clear BYOD Security Policies and Educate Your Employees about Them

One of the greatest dangers required with a BYOD approach is the way that your workers may not be educated on the accepted procedures of staying with your information safe. That is the reason you need particular, clear BYOD security approaches and you have to every now and again teach your workers about said strategies, refreshing and reviving them all the time. Don't simply convey an email to dispatch or help representatives to remember these security

arrangements, either. These approaches ought to be set up amid a far reaching meeting, and general follow-up instructive gatherings ought to be held too. These in-person instruction sessions will enable your workers to get tied up with the possibility that these arrangements are not kidding and ought to be taken after, despite the fact that their own particular gadgets are being utilized.

While considering BYOD security arrangements, make a point to incorporate the accompanying: Try not to permit "jailbroken" gadgets, as these experience the ill effects of known security vulnerabilities.

Any lost or stolen gadgets that have been utilized to get to the organization arrange must be accounted for to IT instantly.

Ensure gadget working frameworks, against malware programs, firmware, programming, hostile to infection programs, and so on. Are stayed up with the latest to keep known vulnerabilities from being misused.

Gadgets used to get to business systems MUST have a screen bolt watchword.

4. Conclusions and Recommendations

In spite of the fact that BYOD permits more prominent adaptability and builds profitability, it significantly affects the customary IT display. Workforce versatility has caused a move in IT consumerisation, where individual gadgets are interfacing with corporate information. While this portability makes various advantages for workers, it likewise puts critical weight on associations. The hardest hit are little and medium associations who don't have the in-house assets and learning to relieve the difficulties. BYOD is an alluring plan of action still there are various security dangers related with it. BYOD security arrangements should be considerably more top to bottom, be that as it may. They ought to incorporate application utilize strategies (what applications are permitted/restricted on gadgets utilized for business), a worker leave methodology (for the individuals who leave the organization), and IT support arrangements (for what happens if representative gadgets utilized for business require support or repair). Focus must also be given on how much right an organization needs to screen and authorize these guidelines, how to actualize them, and that's only the tip of the iceberg.

References

[1] AirWatch. (2012). Enabling bring your own devices (BYOD) in the enterprise. Retrieved from http://www.ciosummits.com/media/solution_spotlight/byod-whitepaper.pdf Google Scholar
[2] AlHarthy, K., Shawkat, W. (2013, November-December). Implement network security control solution in BYOD environment. IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia. Google Scholar, Crossref
[3] Armando, A., Costa, G., Merlo, A. (2013, March). Bring your own device, securely. Proceedings of the 28th annual ACM Symposium on Applied Computing, Coimbra, Portugal. Google Scholar, Crossref
[4] Ballagas, R., Rohs, M., Sheridan, J. G., Borchers, J. (2013). BYOD: Bring your own device. Retrieved from http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf Google Scholar

[5] Björn, N., Sebastian, K., Kevin, O., Stefan, K. (2012). Towards an IT consumerization theory: A theory and practice review. Working papers, ERCIS – European research center for information systems, no 13. Retrieved Febuary 10, 2014 from http://hdl.handle.net/10419/60246 Google Scholar

[6] Chung, S., Chung, S., Escrig, T., Bai, Y., Endicott-Popovsky, B. (2012, December). 2TAC: Distributed access control architecture for "bring your own device" security. ASE/IEEE International Conference on Biomedical Computing, Washington, DC. Google Scholar, Crossref

[7] Cisco. (2012). BYOD: A global perspective (Survey report). Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf Google Scholar

[8] Citrix®. (2013, April). Best practices to make BYOD simple and secure (White paper). Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf Google Scholar

[9] Citrix®. (2012, March). Bring your own devices (Solution brief). Retrieved from http://www.prosysis.com/wp-content/uploads/2013/06/Citrix-BYOD-Solution-Brief.pdf Google Scholar

*Corresponding author.
E-mail address: madhavi.dhingra@ gmail.com