IT Consumerization Innovation & BYODs Risks Mitigation

Rizwan Ahmad
School of Professional Studies, Columbia University, New York
Email: ra2770@columbia.edu
(https://orcid.org/0000-0002-1715-3906)

Abstract - The paper is based on literature review and attempts to discuss what consumerization of IT is and how such consumerization has evolved. The paper further presents an overview of an expansion and usage of BYODs (Bring Your Own Devices) across the world followed by a brief description of its advantages. Further, the paper argues if the consumerization of IT has led to an individual innovative behavior. Subsequently, the paper delves into the risks and challenges associated with it and discuss what those risks and challenges are. Finally, the paper discuss the mechanisms to mitigate security risks and if loopholes around mitigating such risks can be overcome.

Keywords: IT consumerization, BYOD, IT innovation, consumerization, cyber-security, risks mitigation.

I. Introduction

There has been a drastic change in the trend of information technology in the last two decades and the emphasis has shifted from enterprise to consumers (Beimborn & Palitza, 2013). This has generated a drastic increase in the diffusion of mobile devices among the masses as a result of their increased availability and a reduction in prices (Moreno, Tizon, & Preda, 2012). Based on the 19th Americas Conference on information system, approximately 1.2 billion smart phones and tablets were sold in 2012 (Junglas & Harris, 2013) showing how mobile devices have replaced traditional computing methods as a means to access Internet. This has motivated employees "to complete their daily work quickly, efficiently, from anywhere, and in the manner, they choose" (Moreno et al., 2012, pp. 1). This shows how consumerization of IT is trending because of the ubiquitous use of Internet and social media on mobile devices (Fen & LeHong, 2011). Here, consumerization of IT signifies all the IT devices that are privately owned by employees such as laptops, smartphones, and tablets that are "co-used" for business and professional purposes "in addition to being used for original private purposes" (Niehaves, Koffer, & Ortbach, 2012, pp. 1). Gartner (Gartner Press Release, 2012) regards this consumerization as a major IS trend, that has been debated for the past several years, but claims that a major sea of change is yet to come. The consumerization of IT has also been referred to as "bring your own device" (Stagliano, DiPaolo, & Coonnelly, 2013) and is redefining and reshaping relationships between the enterprise IT and employees (Niehaves et al., 2012). However, Castro-Leon (2014) argues that "bring your own device" may also include bring your own applications (BYOAs) that signify privately-owned applications or software that may be co-used for private and business purposes and both these trends are reshaping enterprise IT. However, based on another view, consumerization of IT focuses on the duality of services provided by devices (BYODs) and associated software applications (BYOAs) whereas BYODs solely deals with hardware and BYOAs deals with only software (Harris, Ives, & Junglas, 2012).

Hence some scholars and practitioners may regard BYODs as the only subset of consumerization of IT, whereas others perceive consumerization of IT as having included both BYODs and BYOAs. Based on the discussion above and, for the sake of convenience, I will refer to consumerization of IT as sole BYODs in the rest of the paper where BYOAs is a subset of BYODs.

II. Overview

The emergence of BYOD started in 2003 but it really accelerated in 2011 (Olalere, Abdullah, Mahmod, & Abdullah, 2015). Based on survey conducted by Cisco of 600 US business and IT leaders, 95.00 percent of the respondents said that they allow their employees to use BYODs (Rose, 2013). But based on a survey of 4000 professionals and mobile device users, 41.00 percent of the respondents said that they use their privately-owned mobile devices without taking permission from the company (Kaneshige, 2013b, as cited in Rose, 2013). However another survey points out that 84.00 percent of the respondents use their mobile devices both for the purpose of business and personal use with only 53.00 percent of these respondents claiming that they had password protection on their mobile devices (Business News Daily, 2012, as cited in Rose, 2013). Based on another research, it was found that, in 2017, almost half of the businesses employed BYODs in their business environments. However, based on another survey of 3,796 consumers in seventeen developed and emerging economies conducted by Ovum in 2012, it was found that almost 75.00 percent in emerging economies and almost 44.00 percent in developed economies used their mobile devices for the purpose of business (Olalere et

al., 2015). The figure 1 shows that consumerization of IT or BYODs is a global phenomenon and is becoming prevalent in almost all the major countries, whether developed or emerging.

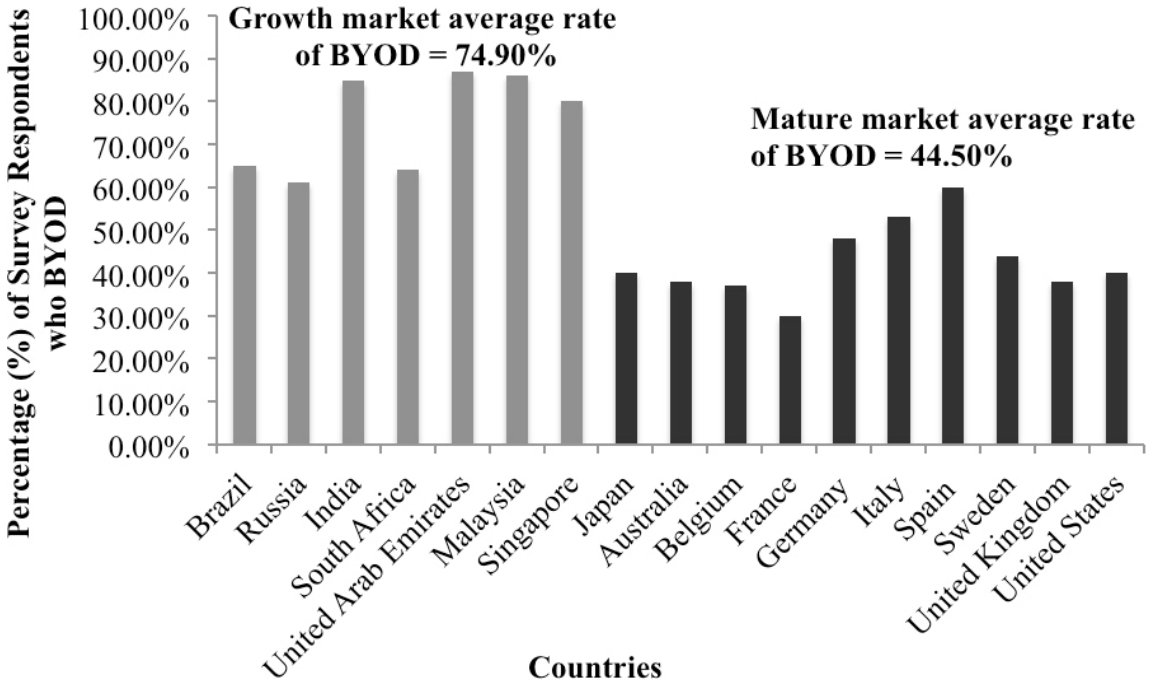

Figure 1. Level of BYOD deployment in both emerging economies and developed economies. Adapted and retrieved from http://www.us.logicalis.com/global/united%20states/whitepapers/logicalisbyodwhitepaperovum.pdf (Ovum, 2012)

With the consumerization of IT, more and more enterprises are allowing their employees to use their personally owned devices to conduct and complete their business task both at the place of their work and outside (Moreno et al., 2012). This clearly explains the blurring of the boundary between business and computer technologies however, at the same time, it has provided employees a sense of responsibility and a way to learn and innovate as Niehaves et al. (2012, pp. 2) puts forth his argument and defines the consumerization of IT as a junction of corporate arrangement of privately-owned technologies and private ownership through which employees "invest their own resources to buy, learn and use consumer technologies at their workplace". This gives a sense of ownership to employees and helps them to innovate even outside their workplace. However, Keyes (2013) argues that cost-reduction on training, hardware and software is another factor in favor of IT consumerization or BYODs.

Moreover, on the positive side, IT consumerization provides employees a sense of mobility, convenience, flexibility that greatly enhances employees' satisfaction and their work performance (Niehaves et al., 2012). Harris (2012) further interviewed IT managers and found that more than 50.00 percent of the respondents believed that employee's satisfaction is a key to enhanced productivity. Furthermore, this trend also provides employees with better user experience and bigger autonomy (Harris & Junglas, 2011) further enhancing their work performance and satisfaction. This makes them use their personal devices for businesses and professional purposes by placing the enterprises' SIM card on their personal mobile devices even if they are not supposed to use it (Holtsnider & Jaffe, 2012). On the negative side, consumerization of IT has many disadvantages such as hazing the boundary between private and business lives, threat to confidentiality, security, loss of control, information protection and increasing complexity (Niehaves et al., 2012). Such security threats have raised a serious concern on the increasing trend of IT consumerization, which has enabled such enterprises to formulate and adopt BYODs frameworks and policies that allows employees to choose the best suitable mobile device based on their needs and assessments both for their personal and business purposes and also to agree on a set of BYODs policies and regulations (Harris & Junglas, 2011).

III. IT Consumerization (BYODs) & Innovation

IT consumerization or to be more precise BYODs are the "most radical shift in the economics of client computing for business since PCs invaded the workplace" (Willis, 2012, pp. 1). It is the new generation of technology-savvy individuals who have triggered this shift and feel more comfortable using their privately-owned devices for the ease of convenience to fulfill their business tasks more efficiently and effectively (Garba, Armarego, Murray, & Kenworthy, 2015). This has enabled the organization to leverage innovation capabilities of employees in the age of consumerization of IT (Koffer, Ortbach, Junglas, Niehaves, & Harris, 2015). With

the emergence of IT consumerization, the costs of hardware are falling gradually and mobile technologies have better and increased functionalities, which aids and abet the IT innovation and helps it to grow even further. This has enabled the employees to empower themselves in order for them to devise and design their own information system, which are as complex as that of the enterprise (Koffer et al., 2015). This new development of such technological setting and user-behavior has upturned the implementation of IT system in the organization, which shows implementation and, hence innovation, has become a bottom-up approach unlike the corporate IT implementation, which was a top-down approach (Crowston et al., 2010, as cited in Leclercq-Vandelannoitte, 2014).

Consumerization of IT has shown a higher degree of user-acceptance and enhanced competence as a result of widely-available array of mobile-devices and associated software applications, which employees may use to self-innovate to create value for the organization (Koffer et al., 2015) unlike corporate IT implementation, which has a relatively low user-acceptance and usage thus creating a "paradox of productivity" (Venkatesh & Davis, 2000, as cited in Leclercq-Vandelannoitte, 2014). Echoing on the same sentiment, Niehaves et al. (2012) argues that employees are competent enough to choose mobile devices and associated software applications best suitable for their business needs and that they are no longer willing for an IT solution to be enforced on them. The emergence of innovative technologies, such as wireless or broadband internet and web 2.0, has greatly reduced the barrier to gaining knowledge by using social media and innovative mobile technologies, which has enabled more and more individuals to use them on their privately owned-devices before devising new ways to use them in the professional set-up (Crowson et al., 2010, as cited in Leclercq-Vandelannoitte, 2014). This shows how such technologies are acclimated by employees first, then solemnized and diffused in the organizational set-up for the purpose of conducting business. Such a bottom-up diffusion has made the organization to rethink about the way they manage, provide and assimilate their user-driven change in their IT infrastructure (Harris et al., 2012; Gartner Press Release, 2012). This shows how the paradigm of IT innovation has shifted from top-down to bottom-up.

Andriole (2012, as cited in Niehaves et al., 2012, pp. 1) argues that "[] there is a reverse technology adoption life cycle at work: employees bring experience with consumer technologies to the workplace and pressure their companies to adopt new technologies". This "reverse adoption" greatly enhances employees' productivity and creativity thus improving organizational performance, which are beneficial to all the stakeholders (Niehaves et al., 2012). Niehaves et al. (2012) clarifies further and discusses the results of the intensive research that has been conducted by various scholars on consumerization of IT and how this approach from bottom – to – top has brought the biggest benefits of innovation potential as a result of IT consumerization. But based on a survey of a worldwide study, Harris et al. (2012) argues that 61.00 percent of business executives perceive the bottom-up diffusion of "organization innovation potential" as a major benefit of IT consumerization. Subsequently, Junglas, Goel, Ives, and Harris (2014) conceptualized this finding by creating an anecdotal link between innovation and IT consumerization and argued that it is very likely for individuals, empowered by IT, to inclulcate the "culture of innovation" through positive changes in work ethos and self-innovation. This prompted another argument about why organization must instill the culture of innovation within every individual in the organization by making them believe that inculcating innovation behavior is their individual responsibility that can not be done away to succeed in the organization (Andriole, 2012, as cited in Koffer et al., 2015), which gives rise to the fact that IT consumerization is the best way to inculcate such innovation behavior. To discuss further the impact of IT consumerization on corporate innovation, Harris et al. (2012) proposes three unique perspectives – Individual, Market & Organizational. These perspectives complement one another but overlaps as well (Koffer et al., 2015).

As regards innovation based on individual workplace, IT expertise, gained by employees in their personal life, can also be used in their professional life as employees are already proficient in keeping themselves up with such technological advances in using new IT tools (Moschella et al., 2004, as cited in Koffer et al., 2015), where expertise denotes proficiency in technology (Amabile, 1996, as cited in Koffer et al., 2015) and self-efficacy in using IT tools (Bandura, 1997, as cited in Koffer et al., 2015). However, another view has also been broadly recognized which defines individual workplace innovation as "intentional introduction and application…. of ideas, products or procedures, new to the relevant unit of adoption, designed to significantly benefit…. the individual, organization or wider society" (West & Farr, 1990, pp. 9). Baskerville (2011) discusses it further and argues that individuals have the proclivity to use and experiment with their personal information system and associated software before choosing the software that are most suitable for them and if they don't feel comfortable using an array of software currently available to them, they invent novel processes to fulfill the existing business tasks leading to innovate business transformation and process. This view has also been recognized by Desanctis and Pool (1994, as cited in Leclercq-Vandelannoitte, 2014) showing the effectiveness of various appropriation moves undertaken by individuals and how such moves shape and reshape by overlapping of technological and organizational innovation through complementary interaction of "technology" and "action". Resonating on the same sentiment, Orlikowski and Hoffman (1997, as cited in

Leclercq-Vandelannoitte, 2014) argues that upcoming technologies always lead to technological changes that are, for most part, opportunity-based and anticipated rising as a result of organizations' needs assessment and "local innovation". This argument assumes that the decision for the placement of such mobile devices rests on top executives and organizational management however another view, without completely disregarding the views of Orlikowski and Hoffman (1997), assumes significance and adds further that the decision to deploy such mobile devices not just rests on the top management but they also be undertaken as a result of the personal initiatives of self-innovation undertaken by employees to enhance organization's operational performance (Goshal & Bartlett, 1994 & Noda & Bower, 1996, as cited in Leclercq-Vandelannoitte, 2014). Now in order to properly understand the implementation of individual innovation, we need to understand the difference between "creativity" and "innovation". Based on the view of Anderson et al. (2012, as cited in Koffer et al., 2015), "creativity" results as a process of individual initiatives and personal "idea generation" whereas "innovation" has a much broader connotation and includes other alternative perspectives as well as the implementation. This explains even further how individual innovation evolves creatively and successively at the workplace through consumerization of IT.

Based on a market perspective, consumer IT is perceived as more reliable, more efficient and simpler as compared to corporate IT (Moschella et al., 2004, as cited in Leclercq-Vandelannoitte, 2014). Drawing on the theory of "learning by doing", Saga and Zumud (1994, as cited in Harris et al., 2012) argues about the post-acceptance stage when employees gain more expertise and become proficient by using IT tools over and over again. So basically they learn while they work. This has created an "ease of use" situations attributed to consumer IT (Harris et al., 2012) for the employees who can use their smartphones or tablets anywhere they wish to or/and even in situations where working without it would almost be impossible (Koffer et al., 2015). This phenomenon of "learning while working" and "ease of use" is recognized widely by Li, Hsieh, and Rai (2013) who argue that such a phenomenon will contribute to positive individual innovation behavior within the organization. As we further see that "[IT consumerization] is the adoption of consumer applications, tools and devices in the workplace – [it] can enhance innovation, productivity and employee satisfaction" (Harris et al., 2012, pp. 99). Hence the notion of higher usage and higher observed usefulness creates a higher relative competitive advantage (Agarwal & Prasad, 1998, as cited in Koffer et al., 2015) as opposed to the usage of corporate IT. Hence it can be argued that the frequency of usage of computer IT tools is directly proportional to individual innovation behavior and increased productivity of employees.

Finally based on organizational perspective, organizations allow personally-owned IT devices because it gives freedom to choose IT tools because of the "relative advantage" or "social influence" (Orbach et al., 2013, as cited in Koffer et al., 2015), which in turn provides autonomy and flexibility to employees as employees don't usually appreciate strict regulations and want to play in choosing to procure and adopt mobile devices (Kettinger & Lee, 2002 & Dell & Intel, 2011, as cited in Koffer et al., 2015) that will be most suitable to them for the purpose of business use. This freedom of choice and fewer restrictions provide them with "job autonomy" (Krause, 2004, as cited in Koffer et al., 2015). Hackman and Oldham (1976, pp. 258) defines "job autonomy" as "the degree to which job provides substantial freedom, independence and discretion to the individual in scheduling the work and determining procedures to be used in carrying it out". This "autonomy" finally leads to "positive, open and supportive behavior" turning finally into individual innovation behavior (Carter et al. 2012, as cited in Koffer et al., 2015). Furthermore, Harris et al. (2012) argues that organizations have higher stakes today and such stakes are rapidly growing exponentially because of the availability of a vast array of affordable privately-owned IT devices with abundance in their functionalities creating a spill-over effect, which is making employees to use the same device for business purpose thus leading to "employee-driven IT revolution". Hence having discussed all the three perspectives – Individual, Market & Organization – they all overlap yet complement each other as it relates to 'flexibility', 'autonomy', 'freedom' and 'productivity' and finally they all lead to individual innovation behavior.

IV. Challenges/Risks Associated With IT Consumerization (BYODs)

Before adopting IT consumerization, organization must take in considerations challenges and risks such as "hidden costs" and "security risks" (Rose, 2013). First of all, the company must decide on providing correct tools and access to company's data to all the employees in order for them to remain productive while keeping the data safe and secured at the same time (Ripley, 2013). Based on a SANS survey for companies taking part in BYODs program, almost half the companies did not know about the type of devices that are assessing their business resources (Johnson, 2012, as cited in Ketel & Shumate, 2014). Another 56.00 percent reported that they did not have appropriate BYODs policy. Furthermore, another 49.00 percent reported that their existing policies barely caught their "basic concerns" (Johnson, 2012, as cited in Ketel & Shumate, 2014). The figure 2 shows the level of challenges or risks associated with BYODs.

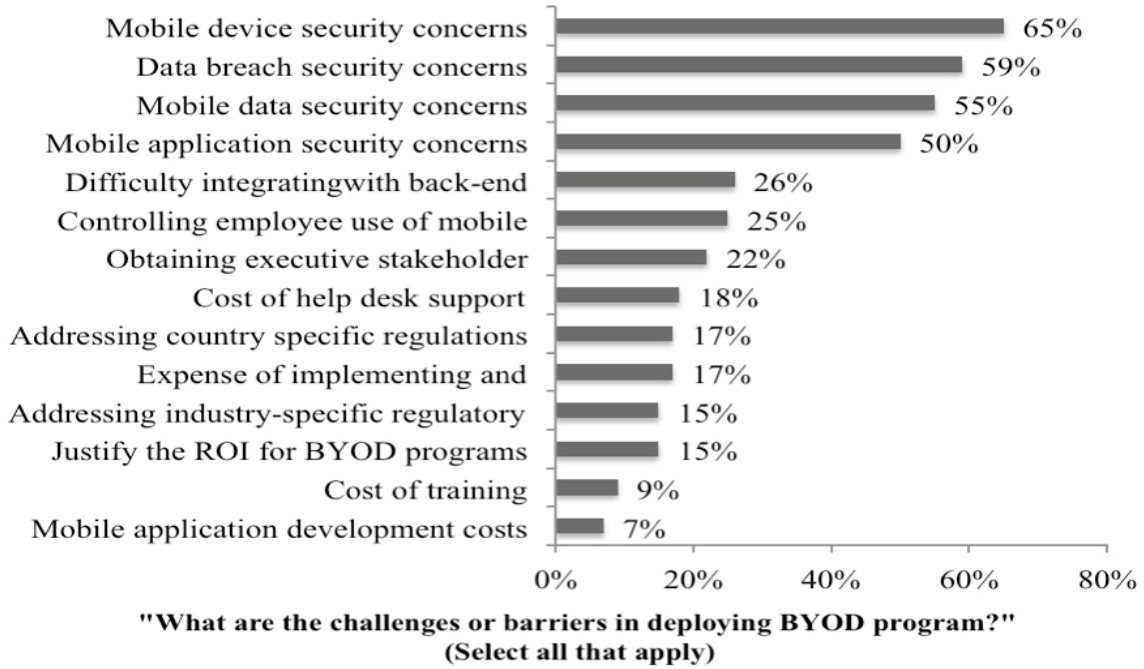

Figure 2. BYOD challenges with security concerns at the top. Adapted and retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/business/whire-papers/wp-forrester_measure-value-of-consumerization.pdf

A. Costs Of Implementing BYODs

Some scholars argue that BYODs bring down the costs considerably (Gallato & Chen, 2014 & Marshall, 2014, as cited in Ogie, 2016). Contrary to this belief, Rose (2013) argues that BYODs actually comes out to be more expensive when we consider the total picture and not just the cost of advice. French, Guo, and Shim (2014) further argues that the company needs to manage diverse platforms and that they need to maintain BYODs solutions, which requires them to purchase various data and voice-service charges for various employees' devices. Then there are other costs such as support costs and application costs. For example, the developers may have to write separate codes for different carrier or version combinations. Similarly, because of the relatively shorter life cycle of mobile programs, the incurred costs are higher. This makes the use of BYODs more expensive. Moreover, Rose (2013) reports that based on Aberdeen group's survey, BYOD approach will cost the company around 33.00 percent more than the company-owned device approach. Aberdeen group further reports "a company with 1,000 mobile devices spends an extra £110,000 ($170,000) per year, on average, when they use a BYOD approach" (Rose, 2013, pp. 66).

B. Security Risks

There are many factors that result in the occurrence of BYODs risks. Based on an industrial report, around 60.00 percent companies suffer from BYODs risks (French et al., 2014). TrustWave, a security vendor, conducted a survey divulging that 90.00 percent of vulnerabilities, that are currently present on the desktop, are also currently present on mobile devices irrespective of the operating system they run on (Olalere et al., 2015). Morrow (2013, as cited in Olalere et al., 2015) identified DDoS (Distributed Denial of Service), Data Leakage and Malware as the most significant security threats. However, Denman (2012), Miller et al. (2012), and Tokuyoshi (2013) elaborated further on security issues and identified

Malware, Data Security and BYOD Network Security as the most prominent security challenge (as cited in Olalere et al., 2015).

1. ***DDoS.*** DDoS attack is an organized and concerted attack on the accessibility of the network system that are introduced through a compromised system thereby increasing the web traffic to such an extent that it does not allow the authenticated employees from running business or personal computing devices on the server (Olalere et al., 2015).

2. ***Data Leakage.*** Depending upon BYODs' policy, employees can access enterprise's data from anywhere, anytime. In the case of theft or loss of their mobile devices, the data may fall into wrong hands and may be intentionally or unintentionally disclosed to the third party (Olalere et al., 2015). If the company owns the device, it can simply remotely wipe the device but if an employee owns it, it may not be possible to remotely wipe the device as there are legal implications to wipe the device because it also contains employees' data (Ketel & Shumate, 2015).

3. ***Malware.*** Malware are those malicious applications or codes embedded within the application. Such malicious codes render corporate applications and mobile devices non-operational and useless (Olalere et al., 2015). With the constant upward growth of mobile devices, there has also been a constant parallel growth in malicious software applications or malware reaching for such devices (Drew, 2012) connecting to corporate resources that has opened up a number of access points and potential targets for cyber-attacks (Johnson, 2012). These malwares hack the organization for the attackers, obstruct business processes and steal business information. There are other types of malware as well such as "key loggers" and "Trojan horses" that can steal password information and capture significant and sensitive business information (WatchGuard Technologies, 2013).

4. ***Unreliable Networks.*** The enterprise has no control over accessing cellular network and Wi-Fi, which privately enabled mobile-devices may use. Such public network is vulnerable to snooping or prying and "Man-in-the-middle-attacks" (Souppaya & Scarfone, 2013).

V. Mechanisms to Mitigate Security Risks

BYODs program can become successful only when it entails various functions such as IT, legal, human resources, finance and operations within an organization (Hayes & Kotwica, 2013). Hence, approach to BYODs' security threat may be taken from non-technical perspectives such as education, awareness and training (Ketel & Shumate, 2015) as well as from technical perspectives**.**

1. Creating BYODs Policy & Compliance

The most important challenge to BYODs' security is unfamiliarity with enterprise's security policies, enterprise's unprotected data, unwillingness on the part of employees to back confidential data etc. (Wang, Wei, & Vangury, 2014). Moreover, because of having various versions of applications and hardware, it is important to design and to re-interpret security policy for each of the mobile platforms, which must be constantly updated (Wang et al., 2014). Echoing on the same sentiment, Mattord & Whitman (2014, as cited in Ketel & Shumate, 2015) argues that employees must be appropriately trained and educated on information security issues in order to counter any such security threat and such training and education must be made compulsory to all the employees and they must be made aware of their personal responsibility of protecting company's assets. Hence, we see that creating a culture of security policy and compliance will help protect the data and information, however it is still may not be easy to implement such regulations (Wang et al., 2014).

2. Mobile Device Management (MDM) Approach

MDM is a centralized solution to managing and monitoring mobile devices in accordance with distinct BYODs policies formulated for each of the organizations (Phiffer, 2012, as cited in Ketel & Shumate, 2015). Because of the BYOD's policy, MDM can take action to redress non-compliance as a result of discovering behavior against "security policies" (Ketel & Shumate, 2015). This creates unnecessary hassle for users as, without analyzing "behavior", MDM "blocks" or sometimes even "resets" the device (Armando et al., 2014, as cited in Ogie, 2016). Further, MDM approach manages security issues in three steps- "Device Management, Security Management & File Synchronization" (Gajar, Ghosh, & Rai, 2013). Ogie (2016) further argues that this approach monitors location, policies, alerts and rules and also includes connection set-up, device registration, passcode, user authentication, compliance and encryption. MDM also restricts the usage of camera and cloud service making the device even more secured (Garba et al., 2015). This creates psychological reluctance to being controlled and monitored because of MDM agent installed on their devices (Koh, Oh, & Im, 2014). This violates user's privacy as well. But MDM's unified approach uses the same tools for all devices and servers, which may be very confusing due to the compatibility issues of different devices. This also makes users loose their flexibility (Garba et al., 2015). Moreover, this unified approach helps create security policies on the whole device or/and whole of the organization thus creating problems for users because of the contradictory policies for different devices or/and if somebody has multiple responsibilities in different organizations (Wang et al., 2014). Further, the application can easily be deleted by users and once deleted, all security settings are removed (Garba et al., 2015). Another major drawback of MDM approach is that a malicious user can initiate data leaks through "abnormal terminal behavior" such as by using faulty accounts or stolen terminals and wireless AP, installed temporarily and illegally (Koh et al., 2014). In the case of loss or theft, MDM has the ability to remotely wipe the device but this may wipe the entire device including his personal data and not just the corporate data (Ketel & Shumate, 2015).

Next, to mitigate the limitation of MDM to discover "abnormal access", Koh et al. (2014) proposed, "dynamic access system based on context" through which, if malicious or abnormal behavior is detected during the use of the network, "dynamic access system" insulates the device and installs the agent. Another approach was proposed by Castro et al. (2013) known as "secured application framework for enterprise" that allows personal and corporate data to be stored separately on the same device, thereby further enhancing the security of the device. Finally, data that are saved on the device must be encrypted with MDM approach so that it cannot be restored in case of loss or theft (Ogie, 2016).

Finally MDM, through the use of Mobile Application Management (MAM), employees' access to certain applications can also be controlled through devising software behavior by "locking down", "securing" and "controlling" specific unapproved applications while rest of the applications on the device remain untouched (Ogie, 2016). Similarly, MDM can also be used, through Mobile Information Management (MIM), to securely share "critical business information" among different platforms having stored them in a central cloud-like service. However, these solutions reduce control over application system (Ogie, 2016).

3. Network Access Control (NAC)

Network Access Control (NAC), by conforming to BYODs policies, protects network "to gain access to resources on the network" by carrying out the authentication process (Ketel & Shumate, 2015). Moreover, NAC solution allows BYODs to connect to network after verifying security traits of mobile devices otherwise it denies access (Ciampa, 2012). It imposes security regulations, obstructs unnecessary traffic, detects non-compliance of the policy and restricts malware (Carr, Snyder, & Bailey, 2010). But Garba et al. (2015) discusses the drawbacks of NAC solution. For example, when single user is using more devices on the network, it might be problematic for the right device to gain an access to "network resources". Similarly, if the device is "malicious", it might go undetected. Such "infected" devices, connected through virtual private network, may compromise the network to which it connects. Finally, there may be mix-up of devices through "logging" and "monitoring" (Garba et al., 2015).

Additionally, MDM approach cannot detect the unauthorized, jail-broken or infected device. Hence to improve security features and for increased "operational efficiency", MDM and NAC approach should be integrated to protect both the network and the device (Orans, 2012 & SANS, 2012, as cited in Ketel & Shumate, 2015).

4. Virtual Network

Virtualization is arguably an effective way to isolate data and space (Wang et al., 2014). Garba et al. (2015) discusses further on virtualization that all the corporate data and applications use space on back-end servers when they run and nothing is stored on BYODs. This makes "viruses" and "malware" not get an access to BYODs because of using "virtualized applications" (Garba et al., 2015). Moreover, in the case of loss or theft, connection is immediately broken and no data is lost. But Garba et al. (2015) also discusses its drawbacks and argues that it takes longer for a virtual application to load than it takes to load a mobile application. Additionally, system requirements are different for different mobile devices and not all such mobile devices meet these requirements (Garba et al., 2015). Further, accessing the remote desktop using BYODs is very challenging and "expose corporate network to external threats" (Garba et al., 2015). Finally, it is difficult to use applications on the small screen that are meant for big screens due to the compatibility issues (Garba et al., 2015). However, virtualization stands out as "privacy friendly" as compared to other approaches especially, MDM approach, since the enterprise does not interfere much with employees' device (Ogie, 2016). Finally to improve the security further in virtual network approach, enterprise must devise a policy to restrict data or file transfer to repudiate "cut-and-paste" and deny printing from the virtual data center (Scarfo, 2012, as cited in Ogie, 2016).

5. Containerization & Dual SIM Approach

Containerization and dual SIM approach is basically used to protect corporate data from being downloaded from "outside work container" (Garba et al., 2015). Similarly, dual SIM approach separates and thus protects "personal" and "corporate" data. Moreover, data loss can be avoided by configuring the device however containerization always leaves "corporate data" on the device and is vulnerable to malware attacks (Garba et al., 2015). Finally in containerization process, it is only the pre-installed application that can be accessed by user and nothing new can be installed after containerization (Garba et al., 2015).

VI. Conclusion

From the perspective of IT consumerization, BYODs have redefined and reshaped IT's role in the corporate world and it has turned out to be a global phenomenon. Based on the literature review, the essay has revealed the correlation between an increasing global trend of IT consumerization and individual innovation behavior incorporating all the three perspectives – Individual, Market and Organizational. This proves that BYODs phenomenon is a function of various issues such as recent technological innovation and the emergence of technologically savvy people, flexibility, convenience and freedom to use such mobile devices from anywhere and anytime. The essay also revealed that IT consumerization leads to enhanced "competence" and enhanced "workload" as a result of "increased autonomy". Finally, the essay also showed how IT consumerization leads to increased individual innovation behavior improving employees' productivity and job satisfaction.

From the perspective of security risks, the essay has revealed many drawbacks in security mechanisms that organizations employ to mitigate such risks. In order to deal with these limitations, organizations must first devise a clear, precise and mandatory BYOD policy such as what devices should be used, how they should be

used and any backup and recovery procedure. The policy must also list all the approved and non-approved applications and the categories of data that should or should not be installed on the device. Hence it is very clear that creating a security culture about the usage of BYODs is extremely important and every employee must be made aware of how important it is to protect company's assets.

Finally, the essay also revealed a number of glitches regarding compatibility issues with various devices and platforms and there is no way to fully address such issues. The essay further found how certain unverified applications could result in introducing malware and viruses resulting in data breach.

From this essay, it is clear that BYODs, as a result of IT consumerization, is expanding globally rapidly but risks and challenges are still not extensively known. Conclusively, there is no mechanism or a combination of mechanisms, as discussed in the essay that will completely eliminate security risks. Implementing BYODs in an organization with adequate security policy may still put corporate data at risks especially when such BYODs implementation is more expensive as compared to traditional IT infrastructure. Future research should delve into employees' perception and behavioral intentions about the effectiveness of BYODs policies and the effectiveness of various security mechanisms employed to greatly reduce security risks.

ACKNOWLEDGEMENT

I would first like to thank Prof. Art Langer of the School of Professional Studies at Columbia University in the City of New York. The door to Prof. Langer's office was always open whenever I ran into trouble or had a question about my research and writing. He consistently allowed this paper to be my own work, but steered me in the right the direction whenever he thought I needed it.

I would also like to thank Prof. Chrisanthi Avegrou of the Department of Management at London School of Economics & Political Science. Without her passionate participation and input, the essay could not have been successfully completed.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Finally, I must express my very profound gratitude to my parents and to my siblings for providing me with unfailing support and continuous encouragement through the process of researching and writing this paper. This accomplishment would not have been possible without them.

DECLARATION OF INTERESTS STATEMENT

The author has no conflicts of interest to declare.

References

[1] Baskerville, R. (2011). Design theorizing individual information systems. In *Proceedings of the Pacific Asia conference on information systems* (pp. 1-13). Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1024&context=pacis2011 Last Accessed June 05, 2018

[2] Beimborn, D., & Palitza, M. (2013). Enterprise app stores for mobile applications – development of a benefits framework. In *Paper presented at the Nineteenth Americas Conference on Information Systems*, Chicago, IL.

[3] Carr, H., Snyder, C., & Bailey, R. (2010). *The Management of Network Security*. Upper Saddle River, NJ: Prentice Hall.

[4] Castro, P.C., Ligman, J.W., Pistoia, M., Ponzo, M., Thomas, G.S., Wood, S.P., & Baluda, M. (2013). Enabling-bring-your-own-device using mobile application instrumentation. *IBM Journal of Research and Development, 57*(6), pp. 7:1 – 7:11. doi: https://doi.org/10.1147/JRD.2013.2279640

[5] Castro-Leon, E. (2014). Consumerization in the IT Service Ecosystems. *IT Professional, 16*(5), pp. 20-27. doi: http://doi.org/10.1109/MITP.2014.66

[6] Ciampa, M. (2012). *Security + Guide to Network Security Fundamentals* (4th Edition). USA: Cengage Learning.

[7] Drew, J. (2012, August 1). Managing Cybersecurity Risks. *Journal of Accountancy, 214*(2), pp. 44-48. doi: https://www.journalofaccountancy.com/issues/2012/aug/20125900.html

[8] Fenn, J., & LeHong, H. (2011). *Hype cycle for emerging technologies* (Rep. No. G002156500). Stamford, CT: Gartner. Retrieved from https://www.gartner.com/doc/1754719/hype-cycle-emerging-technologies- Last Accessed June 03, 2018.

[9] Forrester . (2012). *Key strategies to capture and measure the value of consumerization of IT.* Cambridge, MA: Forrester Consulting. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf Last Accessed June 05, 2018

[10] French, A.M., Guo, C., & Shim, J.P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems, 35*(1), pp. 191-197. doi: https://doi.org/10.17705/1CAIS.03510

[11] Gajar, P. K., Ghosh, A., & Rai, S. (2013). Bring Your Own Device (Byod): Security Risks And Mitigating Strategies, *Journal Of Global Research In Computer Science, 4*(4), pp 62-70. Retrieved from http://www.rroij.com/open-access/bring-your-own-device-byod-security-risks-and-mitigating-strategies-62-70.php?aid=38224 Last Accessed June 06, 2018

[12] Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environment. *Journal of Information Privacy & Security*, *11*(1), pp. 38-54. doi: https://doi.org/10.1080/15536548.2015.1010985

[13] Gartner Press Release, Newsroom (2012, November 6). *Gartner says 821 Million Smart Devices Will Be Purchased Worldwide in 2012. Sales to Rise to 1.2 Billion in 2013.* [Press Release]. Barcelona, Spain. Retrieved from https://techcrunch.com/2012/11/06/gartner-1-2-billion-smartphones-tablets-to-be-bought-worldwide-in-2013-821-million-this-year-70-of-total-device-sales/ Last Accessed June 03, 2018

[14] Hackman, J.R., & Oldham, G.R. (1976). Motivation through the design of work: test of a theory. *Organization Behavior and Human Performance, 16*(2), pp. 250-279. doi: https://doi.org/10.1016/0030-5073(76)90016-7

[15] Harris, J.G., & Junglas, I. (2011). *The Promise of Consumer Technologies in Emerging Markets* (pp. 1-11, Rep.). Accenture Institute for High Performance. Retrieved from https://www.finyear.com/attachment/321146/ Last Accessed June 04, 2018
[16] Harris, C. (2012). *Mobile consumerization trends & perceptions: IT Executives and CEO Survey* (pp. 1-8). New York, NY: Decisive Analytics, LLC. Retrieved from https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf Last Accessed June 04, 2018
[17] Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: When Gadgets turn into Enterprise IT tools. *MIS Quarterly Executives*, *11*(3), pp. 99-112. Retrieved from https://www.researchgate.net/publication/292896935_IT_Consumerization_When_Gadgets_Turn_Into_Enterprise_IT_Tools Last Accessed June 03, 2018
[18] Hayes, B., & Kotwica, K. (2013). *Bring your own device (BYOD) to work: Trend report*. Elsevier. CrossRef
[19] Holtsnider, B., & Jaffe, B. (2012). *IT Manager's Handbook: Getting Your New Job Done*. Waltham, MA: Morgan Kaufmann. Retrieved from https://www.oreilly.com/library/view/it-managers-handbook/9780124159495/ Last Accessed June 04, 2018
[20] Johnson, K. (2012). *SANS mobility/BYOD security survey* (pp. 1 – 15, Rep.). SANS Institute Whitepaper. Retrieved from http://www.webtorials.com/main/resource/papers/mobileiron/paper3/Mobility_BYOD_%20Security_Survey.pdf Last Accessed June 06, 2018
[21] Junglas, I., & Harris, J. G. (2013). The Promise of Consumer Technologies in Emerging Markets. *Communications of the ACM*, *56*(5), pp. 84-90. doi: https://doi.org/10.1145/2447976.2447995
[22] Junglas, I., Goel, L., Ives, B., & Harris, J.G. (2014). Consumer IT at work: Development and test of an IT empowerment model. In *Proceedings of the 35th international conference on information systems* (pp. 1-19). Auckland. Retrieved from https://pdfs.semanticscholar.org/7b35/742565bc3efacf1cfaa11d71c5a00995fc2b.pdf?_ga=2.42120805.1191916195.1554058872-1851627392.1549902694 Last Accessed June 05, 2018
[23] Ketel, M., & Shumate, T. (2014). Bring Your Own Device: Benefits, Risks & Control Techniques. In *IEEE SoutheastCon 2014*. Lexington, KY: IEEE. doi: https://doi.org/10.1109/SECON.2014.6950718
[24] Keyes, J. (2013). *Bring your own device (BYOD) survival guide*. Boca Raton, FL: CRC Press. Retrieved from http://www.ittoday.info/Excerpts/BYOD_Survival_Guide.pdf Last Accessed June 04, 2018
[25] Koffer, S., Ortbach, K., Junglas, I. A., Niehaves, B., & Harris, J. (2015). Innovation Through BYOD? The influence of IT Consumerization on Individual IT Innovation Behavior. *Business & Information System Engineering, 57*(6), pp. 363-375. doi: https://doi.org/10.1007/s12599-015-0387-z
[26] Koh, E.B., Oh, J., & Im, C. (2014, March 12-14). A study on security threats and dynamic access control technology for BYOD, Smart work environment. In *Proceedings of International MultiConference of Engineers and Computer Scientists*, Vol. II. Hong Kong: IMECS. Retrieved from http://www.iaeng.org/publication/IMECS2014/IMECS2014_pp634-639.pdf Last Accessed June 06, 2018
[27] Leclercq-Vandelannoitte, A. (2014). Interrelationships of identity and technology in IT assimilation. *European Journal of Information Systems, 23*(1), pp. 51-68. doi: https://doi.org/10.1057/ejis.2013.16
[28] Li, X., Hsieh, J.J.P.A., & Rai, A. (2013). Motivational differences across post-acceptance information system usage behaviors: an investigation in the business intelligence systems context. *Information Systems Research, 24*(3), pp. 659-682, 879-881. doi: https://doi.org/10.1287/isre.1120.0456
[29] Moreno, C., Tizon, N., & Preda, M. (2012). Mobile Cloud Convergence in GaaS: A Business Model Proposition. In *45th Hawaii International Conference on System Sciences* (pp. 1344-1352). NewYork, NY: IEEE. doi: http://doi.org/10.1109/HICSS.2012.433
[30] Niehaves, B., Koffer, S., & Ortbach, K. (2012). IT consumerization – A theory and practice review. In *proceedings of the 18th Americas Conference on Information Systems* (pp. 1-9, Paper 18). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.9359&rep=rep1&type=pdf Last Accessed June 03, 2018
[31] Ogie, R. (2016, January). Bring Your Own Device. An overview of Risk Management. *4 IEEE Consumer Electronics Magazine, 5*(1), pp. 114-119. doi: https://doi.org/10.1109/MCE.2015.2484858
[32] Olalere, M., Abdullah, M.T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. Sage Open, 5(2), pp. 1-11. doi: https://doi.org/10.1177/2158244015580372
[33] Ovum. (2012). An emerging market trend in more ways than one (Consumer impact technology). Retrieved from http://www.us.logicalis.com/global/united%20states/whitepapers/logicalisbyodwhitepaperovum.pdf Last Accessed June 04, 2018
[34] Ripley, C. (2013, May 17). *Take advantage of BYOD without sacrificing security*. PCWorld. Retrieved from http://www.pcworld.com/article/2038163/take-advantage-ofbyod-without-sacrificing-security.html Accessed from June 05, 2018
[35] Rose, C. (2013). BYOD: An examination of bring your own device in business. *Review of Business Information System, 17*(2), pp. 65-70. doi: https://doi.org/10.19030/rbis.v17i2.7846
[36] Souppaya, M., & Scarfone, K. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (pp. 1-21) (USA, US Department of Commerce) Gaithersburg, MD: National Institute of Standards and Technology (NIST). doi: http://dx.doi.org/10.6028/NIST.SP.800-124r1
[37] Stagliano, T., DiPoalo, A., & Coonnelly, P. (2013). Consumerization of Information Technology. *Graduate Annual*, *1*(10), pp. 1-43. Retrieved from https://digitalcommons.lasalle.edu/graduateannual/vol1/iss1/10 Last Accessed June 03, 2018
[38] Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. In *2014 IEEE 11th Consumer Communications and Networking Conference(CCNC)* (pp. 80-85). Las Vegas, NV: IEEE. doi: https://doi.org/10.1109/CCNC.2014.6866552
[39] WatchGuard Technologies. (2013, January 28). *Ten tips for establishing a secure foundation for BYOD*(pp. 1-8, Rep.). WatchGuard Technologies Whitepaper. Retrieved from https://ro.uow.edu.au/eispapers/5418/ Last Accessed June 06, 2018
[40] West, M.A., & Farr, J.L. (1990). Innovation at work. In M.A. West and J.L. Farr (Eds), *Innovation and creativity at work: Psychological and organizational strategies* (pp. 3-13). Chichester, England: Wiley. CrossRef
[41] Willis, D. A. (2012). *Gartner publishes Bring your own device: New opportunities, new challenges report* (Rep. No. G00238131). Gartner. Retrieved from https://www.gartner.com/doc/2125515/bring-device-new-opportunities-new Last Accessed June 04, 2018