# Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD).

Felix. C. Aguboshim[1] and Joy. I. Udobi[2]

[1]Principal Lecturer, Department of Computer Science, Federal Polytechnic, Oko Nigeria.

felixaguboshim@gmail.com

[2]Principal Lecturer, Department of Mathematics/ Statistics, Federal Polytechnic, Oko Nigeria.

joyis4jesus2yahoo.com

**Abstract**

The use of employee-owned mobile devices such as smart phones, tablets, laptops, etc., to access business enterprise content or networks otherwise referred to as of 'Bring Your Own Device' (BYOD) has further made the confidentiality, integrity, and availability of organizations' data become insecure, and prone to breaches and fraudulent activities. In this study, the authors explored a narrative review that focuses on the theoretical underpinnings of vast works of literature that revealed significant information on the conceptual framework, existing systems that adopt BYOD security, analysis, and synthesis of prior research. Using some keywords "BYOD system security", "BYOD security threats", "cyber-attacks and security", etc., an electronic database search extracted peer-reviewed articles from the last five years. The thematic analysis of fifty-one articles retrieved revealed that breaches and fraudulent activities exist with the use of BYOD that may be perpetrated against organization's data, intentionally or maliciously. Good policies and guidelines on the use of BYOD coupled with good formulation and communication of same, should be adhered to avert some forms of security breaches. There is the need to preserve user's privacy, organizations' data confidentiality, integrity, and availability, and secure same in the devices of employees using their own devices to process corporate and personal data, by using acceptable and effective BYOD Policy and Mobile Device Management Solution (MDMS). This may increase mutual trust and BYOD adoption rate, new innovations and influence that can positively impact the organizations and their employees.

**Keyword:** *BYOD, security threats, password, cyber-attacks and security, Information security.*

**DOI**: 10.7176/JIEA/8-1-07

## 1. Introduction

Bring your own device (BYOD) is a system where employees are allowed to use their mobile devices anywhere to access privileged organization data. BYOD can be implemented by allowing usage of employee owned devices or by companies buying mobile devices for the employees (Kumar, 2014). In this paper, the authors addressed justifiably concern among IT organizations on the security risks and data leakages inherent in Mobile Electronic Transactions (MET). MET includes (but not limited to) the use of employee-owned mobile devices such as smart phones and tablets to access business enterprise content or networks otherwise referred to as of 'Bring Your Own Device' (BYOD). MET that employs BYOD policy effectively, no doubt, can result to businesses benefits, encourage job satisfaction among employees, cause better job efficiency and flexibility. Also, there is cost savings through BYOD as a result of initial device purchase, on-going usage, and IT helpdesk support since employees bring their own devices for use by their employers. However, allowing employees to use their own devices to access company information gives rise to a number of issues that a business must answer in order to comply with its data protection obligations. To address this issue, many organizations are turning to Mobile Device Management (MDM) products and services. However, many IT organizations wanted organizations to focus on managing the data rather than the devices, while others believe that the focus should be more on users rather than on devices. This paper therefore focuses on the data and the user with the aim to address the increased potential for data leakage and security challenges associated with MET exemplified by BYOD policies. The main objective of this study was to inform IT, managers of organizational security function, the strategies to withstand most security threats, vulnerabilities, and risks associated with BYOD systems

The Information Technology (IT) Consumerization and Bring Your Own Device (BYOD) trend are changing the enterprise work environment platform. Many organizations have embraced BYOD because of its perceived benefits in terms of increase productivity and efficiency, and the decrease of administrative costs (Bradley, Loucks, Macaulay, Medcalf, & Buckalew, 2013). However, BYOD, coupled with consumer devices, mobile applications, cloud computing technology, and technology savvy employees put together provide a perfect example of disruptive technology for organizations' Information Technology (Garba, Armarego, Murray, & Kenworthy, 2015). This culminates in a computerization process shift in the sense that employees use their IT driven technology to complete their job-related activities (Baskerville, 2011) within and outside the organizations' premises. Subsequently, the IT technology adoption logics are disrupted and reversed (Nan, 2011) because instead of the IT department driving the innovation within the enterprise, the push comes from the outside through the consumers (Dernbecher, Beck, & Weber, 2013). This disruptive technology is posing various challenges to organizations that decide to embrace BYOD in addition to the consequences they may face. Few organizations have proactively and effectively elaborated strategies to address challenges and consequences (Harris, Ives, & Junglas, 2012). For instance, policy gaps are the foundation of most security failures and BYOD security is no exception (Zahadat, Blessner, Blackburn, & Olson, 2015). Besides, employee non-compliance to policy and mainly personal mobile devices cause directly or indirectly over 50% of all information system security violations (Son, 2011). The general IT problem is that instituting a BYOD program not also increases the organization's exposure to information system security risk but put the organizations in situation where they struggle to tackle effectively and proactively the challenges and aftermaths of the BYOD adoption. The specific IT problem is that some CIOs lack strategies to adapt an organization's information system to support BYOD.

## 2. Conceptual Framework

We adopted the Unified Theory of Acceptance and Use of Technology (UTAUT) as a conceptual framework for this study. UTAUT was proposed by Venkatesh, Morris, Davis, & Davis (2003) and supposed that the benefits of using a technology and the factors driving the decision to use it, determine the individual's acceptance behavior. The theory considers factors that influence behavioral intention and use behavior of technology. Based on the model, both user adoption and usage of IT are affected by four constructs: performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC) and four moderators: gender, age, experience and voluntariness of use (Venkatesh, et al., 2003). These constructs and moderators affect the Behavioral Intention, that is, the user's thoughts and plans of using new technology and finally the using itself, Use Behavior. (Venkatesh, et al., 2003). UTAUT model in recent times has been widely adopted (Oye, AIahad, & Abrahim, 2014). Some researchers' attention have been drawn to the usefulness of the model, and to adopt the model to investigate adoption of mobile innovations (Loose, Weeger, & Gewald, 2013; Arumugam, Yahya, Rozalina, & Mohd, 2014; Zhou, Lu, & Wang, 2010).UTAUT has been adopted to understand the factors behind future young employees' BYOD adoption by investigating the consumerization drivers of BYOD service adoption among future employees (Bhattacherjee, Limayem, & Cheung, 2012), and the attractiveness of a company for future employees and the BYOD service adoption (Dernbecher, et al., 2013; Siciliano,2014).Unified Theory of Acceptance and Use of Technology (UTAUT) was adopted as our theoretical foundation to study security issues associated with BYOD, and the pros and con of its consumerization implications.

## 3. Methodology

A narrative review approach was adopted in this study to review significant information on the conceptual framework, existing systems and policies that enhance BYOD security, analysis, and synthesis of prior research. According to Hill and Burrows (2017), a narrative review is adopted where summaries of different primary studies from which conclusions may be drawn into a holistic interpretation contributed by the reviewers' own experience, existing theories and models are needed.A narrative study approach is best suited to a study that can be described as descriptive or explanatory (Bell, 2017; Privizzini, 2017). Results from narrative studies are of a qualitative rather than a quantitative meaning (Scarnato, 2017). The strengths of narrative study are in its ability to comprehend the diverse and numerous understanding around scholarly research topics and the opportunity to speak with self-knowledge, reflective practice and acknowledgement of shared views and knowledge (Malcolm, 2017). Researchers with diverse understandings have co-opted the concept of narrative reviews as best suitable for comprehensive topics and have used narrative inquiry or narrative research to name their methodology (Caine, Estefan, & Clandinin, 2013; Rutherford, 2017). In this paper, we lay out more clearly the methodological commitments of narrative inquiry. Within narrative inquiry, we have made the search criteria and the criteria for inclusion explicit. Our review process included key words and term identification, article identification, quality assessment, data extraction, and data synthesis. Methodological triangulation is the use of multiple sources of data that pertains to a case or phenomenon, to gain multiple perspectives, maximize reliability and validation of data and build coherent justification of data interpretation (Durif-Bruckert, et al., 2014). We adopted methodological triangulation to ensure the reliability and validity of data, and justification of interpretations from the reviews.

## 4. Data Collection

This review was based on a literature search of online information obtained from the following international library databases: the ProQuest databases, ScienceDirect, Walden University collection of scholarly and peer-reviewed journals, and other related texts. A combination of phrases and terms were used as key search words in the databases for related literature on security issues on mobile IT and BYOD technology. Such phrases and terms included *IT consumerization, consumerization of IT, UTAUT, technology acceptance model, technology adoption, BYOD, BYOT, CYOD, and CYOT, security issues with BYOD, cyber-attacks and security, Information security,* and many others. We conducted a thorough review of the literature and incorporated 51 references into our study. Fifty (98%) of total references incorporated in the study are peer-reviewed, while (70%) are peer-reviewed journals that are within the last 5 years. A summary of these sources is given in Table 1.

Table 1 *Summary of Research Articles Consulted in the study*

| Sources from review of the professional and academic literature | Number |
|---|---|
| Total references in the study review: | 51 |
| Total peer-reviewed references in the study: | 50 |
| Total peer-reviewed in the study w/in 5 year: | 35 |
| % Peer-reviewed references in the study: | 98% |
| % Peer-reviewed references in the study w/in the last 5 years: | 70% |

### 4.1 Analysis and Synthesis of Prior Research

Over the years there have been enormous advances in the field of technical information security controls with complex and matured technical controls such as anti-virus, client-based firewalls, and real-time patching (Stewart & Lacey, 2012). Some socio-technical trends that are likely to shape the cybersecurity environment in the next decade have been identified (Dupont, 2013), and their possibility to produce a great effect in the information security technical controls observed (Hinduja & Kooi, 2013). In the last decades, the IEEE Security & Privacy has focused on a wide variety of important policies that have not only contributed to the understanding of security, but also to the innovative and effective solutions to information technology security problems (Pfleeger, Predd, Hunker, & Bulford, 2010). These trends, according to Dupont (2013), are cloud computing; big data (Hartzog & Stutzman, 2013); the Internet of Things; the mobile internet or mobile computing; brain-computer interfaces, mobile robots; quantum computing, and the militarization of the internet. These trends come with their challenging needs and requirements for more data, more connections, more movement, and flows. As a result of this massive data storage and interconnectivity, organizational data and information are exposed to more opportunities for malicious exploitation and threats, less security, and less control (Montesino & Fenz, 2011). The occurrence of disasters, operation errors, and oversights, further increase the risks placed on information systems.

Much prior research has also focused on individual fraud types: identity theft, intellectual property fraud or insurance fraud. However Scholarly research in the area of fraud is difficult (Goode & Lacey, 2011). Studies of financial fraud are hampered because it is difficult, if not impossible, to access offenders. Firms may be reluctant to admit experiencing security or fraud problem within their operations, while managers may resist inquiry or analysis from outside groups, including academic researchers to study their firms for fear of exposing their reputation to the public. It is also difficult for external researchers to gain access to the organization's original, un-sanitized data. This is one of the reasons why determining what contributes to information insecurity has proven to be complex in nature because such activities required to handle threats to the organizations' data: confidentiality, integrity, and availability are also complex (Fenz, Heurix, Neubauer, & Pechstein, 2014).

Despite the implementation of advanced security technical controls, information systems have remained vulnerable. This is because there is evidence that suggests that human vulnerabilities are increasingly exploiting information systems (Stewart & Lacey, 2012). Some researchers have noted a number of reasons for this, ranging from problems with the usability of information systems (Hartzog & Stutzman, 2013; Cristian & Volkamer, 2013; Okesola & Grobler, 2014), compromised decisions by users (Greavu-Serban & Serban, 2014) and limited ability to comply with Knowledge Management Systems or instructions (Shehata, 2015; de Albuquerque & dos Santos, 2015). However, Dwivedi, et al. (2015) summarized and categorized these mistakes into four categories: process (management process and technical project management methodologies), people involved in a project, product (project size and urgency, including its goals, performance, robustness, and reliability), and technology (IS failures resulting from the use and misuse of modern technology). Nevertheless, Study by Ho, Hsu, and Yen (2015) has provided an improvement strategy to manage the Information Security Management (ISMS) of the organization by proposing three core control items of the Information Security Management (ISMS) namely security policy, access control, and human resource security.

### 4.2 Analysis of Pros, Cons, and Risks of Implementing BYOD Policy in an Organization.

Allowing personally owned devices to access the organization network can lead to privacy and data security breaches, as personally-owned devices may lack the necessary protections and features. However, BYOD has the potential to significantly reduce capital expenditures, though it can dramatically increase operating expenditures if not properly deployed and managed. There is cost savings on the part of the employer if employees own the mobile device and the organization reconfigures it for business use, otherwise the reverse is the case. If that is the case, the organization saves on buying the devices. Overall productivity increases because the employee can work from anywhere. Companies with a solid BYOD system in place tend to attract better employees because it brings restriction on private emails, videos and websites (EYGM, 2013). This also brings better productivity as cost is being save on unnecessary use of internet by employees.

Major risks are centered on the security of the company's data. Implementation therefore differ slightly depending on who owns the mobile device. Where the company provides the device, as is most likely the case, risk measures may include blocking installations of things that are distracting, secret software to see what the employee does on the device, and possibly restrict private use of the devices.

Culture is a subjective phenomenon that refers to the shared values among members of a group or organization. To have a good organizational culture one **must teach it, define it, live it,** measure **it, and reward it.** So, the criterion for judging and analyzing the challenges of addressing both an organization's culture and the culture of the hosting country is to determine what extent to which it goes on the same track with the tasks or vision of the organization. Organizational culture is a double-edged sword that serves as the platform for facilitating and reaching the organizational goals. On the other hand, it can be a barrier on the edge of change.

Organizations must endeavor to run their vision irrespective of conflict cultural setup. a global organization must dictate a set of professional guidelines or vision in all their organizations. Professional guidelines in all their organizations must not change. However the organization may adjust to the cultural settings of the culture they live in while maintain their vision of professional guidelines. . If you do not guide the culture, the culture will guide you (Jahanian & Salehi, 2013).

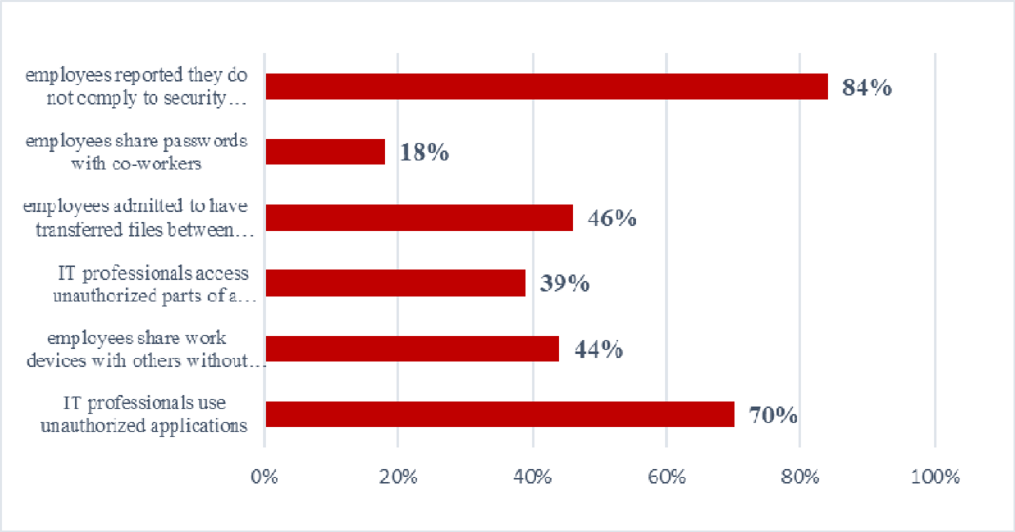
### 4.3 Security Issues inherent in BYOD Transactions

The adoption of BYOD like laptops, Smartphone, tablets, etc as primary computing endpoints, by enterprises, has continually been on the increase (MobileIron,2012).As mobile users now manifest access over a wide range of contents from behind the firewall, or from email to corporate repositories, new challenges that increase the risk of data loss are also manifested. As BYOD in the workplace continues to be on the increase, potential legal and data protection risks also rise warranting the obvious need for businesses to think carefully about BYOD so as to provide appropriate and effective policies and countermeasures against these risks inherent in BYOD.A data breach or leakage results when sensitive or confidential data of an organization is copied, transmitted, viewed, stolen or used by an unauthorized individual (Shabtai, Elovici, & Rokach, 2012). Data leakage is applicable to both data at rest, on the disk, in transit, and various other internet channels. The increase of mobile technology also brought about an increase in data leakage whether by accident or malice. It is believed that substantial data leakage results from within activities though the threat from outside the corporation is still a concern. Threats also come virtually from every employee because every device that stores company information is a potential threat. A lost device can result in a threat to data leakage since such lost laptop can be recovered by one with malicious intent. Data leakage could also result from lack of awareness that put employees into behaving in an unsafe manner.

Despite this attending challenges, companies have continued to allow the use of personal mobile devices and corporate apps basically for the users satisfaction, the difficult to impose usage restrictions notwithstanding. Mobile devices have lots of storage that can potentially be stored locally on the device. They also have facilities for persistent cloud-connectivity with data services, such as Dropbox, and devices that can connect constantly to any available network whether it is trusted by the enterprise. Again, mobile devices are easy to move data from the device to clouds outside enterprise control. As a result, it has also become increasingly difficult to use mobile devices in a secure way that can prevent data leakage (MobileIron, 2012). Data leakage according to Purohit and Singh (2013), can be classified into three levels: unintentional leak, intentional leak, and malicious leak. Intentional Leak includes document rename, document type change, partial data copy, and remove keyword (Purohit &Singh, 2013). The third classification of data leakage called Malicious Leakage usually occurs when a user deliberately sneaks the confidential data past the security rules. Malicious data leakage is a sneak through character encoding, print screen, password protected, self-extracted archive, hide data and policies or product. A compromise of integrity involving the disappearance or damage, in which a correct data copy is no longer available to the organization (Liu &Kuhn, 2010).

In two surveys conducted by CISCO in 10 countries of different social and business cultures, comprising 100 end users and 100 IT professionals selected from each of these 10 countries, results from the research, as shown in the tables 1 and 2, discovered that despite the security established plans and programs including operational and tools currently in place by the companies, employees still behave in a risky manner likely put the corporate and personal data at security risk.

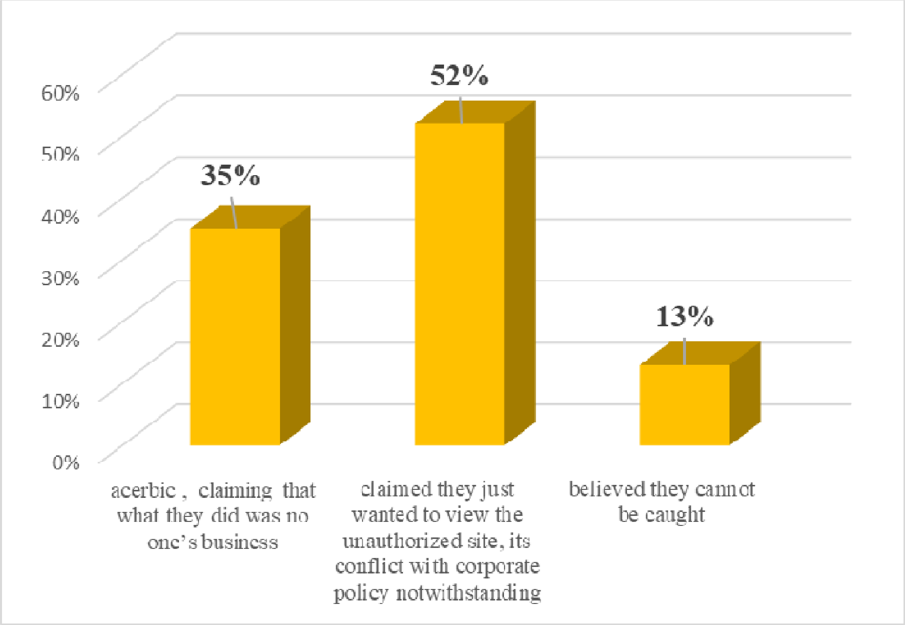
**Figure 1.** *Percentage employees that still behave in a risky manner despite the security established plans and programs*



Source: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf

Results show that 70 percent of IT professionals use unauthorized applications that has resulted in as much as half their company's data loss incidents. 44 percent of employees share work devices with others without supervision. 39 percent of IT professionals' access unauthorized parts of a company's network or facility. 46 percent of employees admitted to have transferred files between work and personal computers when working from home. 18 percent of employees share passwords with co-workers with China, India, and Italy topping this proportion with 25 percent (CISCO, 2008). The result confirmed most end users in one of the countries under study use email and instant messaging for their personal use resulting in their changing of the company's IT security settings to enable them view unauthorized websites. According to the result of the survey, only 16 percent of employees reported they comply to security policies all the time. Another study according to (Symantec, 2015), has revealed that 2 out of 5 employees download work files to their personal smartphones and tablets. Therefore then, employees' behaviors with their mobile devices significantly put to corporate and personal data at varied security threats and data leakage.

**Figure 2**. *Employees' reason for putting cooperate data at risk or tempering with security settings according to CISCO (2008).*



Source: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf

As evident from Table 2, employees' reason for putting cooperate data at risk or tempering with security settings according to CISCO (2008), included a 35 percent group whose reasons were so acerbic, claiming that what they did was no one's business. About 52 percent claimed they just wanted to view the unauthorized site, its conflict with corporate policy notwithstanding, while 13 percent believed they cannot be caught while performing unauthorized activities. Other reasons for putting corporate data at risk was purely monetary because it appears pretty cheaper to use the computer supplied by an employer for a family or household use particularly in a situation where cultures compelled extended families to live together. Some employees do not understand the security policy operational in their work environment.

### 4.4 Countermeasures

Countermeasures should begin with the careful analyses of the factors that might be responsible for employee behavior and whether or not the associated risks was attributable to factors relating to electronic transactions. Where these factors responsible for data leakage hinge on ignorance, defiance, or simply lack of caring by employers, solution to securing corporate data could come through appropriate literacy programs that will make for appropriate investments in security technology. Employees should be taught that corporate data is essentially money, and corporate data leaking simply means throwing money away and allowing outsiders, who pose the biggest threat, to pick it up and use same against you. Employees should be trained to cooperate and be at ease with the company's lay down security policies to help implement security directives. Avenues should be created through training that will inculcate in the employees the appropriate security organization for reporting suspicious behavior, security threat incidents and recognizable attacks. However, training of employees alone is not enough, it is sufficient to apply some realizable steps and tools that can prevent data leakage and track data's movement capable of indicating where data are stored, accessed , and used. Also types of data that require specific protection within and beyond the company's walls must be appropriately identified. Aside, it is most important to consider new security approaches involving next-generation tools and capabilities.

To quickly identify data loss prevention practices considered as best is a complex issue (Liu & Kuhn, 2010). However, every organization is expected to leverage best practices and identify data loss prevention solution that best suits their specific needs. This can be achieved by identifying all the various potential data loss modes, like the one enumerated above, and then prioritizing them based on criteria such as past leakages, the chances of having a breach, and the number of users / devices applicable to those modes identified. In all mobile DLP (Data Leakage Prevention) and mobile content collaboration offer the best countermeasures (ZENPRISE_DLP, n.d.), that will protect data with the following mobile data management best practices (Magalhaes, 2011).

They include

- Provision of a secure platform for all file types.
- File synchronization across mobile devices including back-end apps.
- Enterprise collaboration tools and content integration.
- Data Encryption whether or not data are in transit
- Control of content version and time expiry
- context-aware policies for iOS for actions requiring “save”, “print”, “email”, “email link”, and “copy/paste”.
- Online policies that wipe container upon device jailbreak or failed login attempts
- Facility for data wipe when an employee left the organization etc.

Security management solution that meets the business requirements including tools, processes, and policies required to implement the solution exits. Mobile device management (MDM) solutions is entrenched with basic device lifecycle management abilities and capabilities that offer simple device provisioning like lock, and wipe. MDM software has become an unavoidable tool for IT to gain control over BYOD among enterprises (Zenprise_MDM, n.d.). MDM now offers security beyond the device and across all major platforms of iOS, Android, BlackBerry, Symbian, and Windows Mobilewhich is a good work now that mobile devices are increasingly being used in cooperate enterprises. MDM makes use of a centralized visibility that makes all deployed devices visible to the corporate network so as to manage the devices by applying the right set of policies compliance. For example, unmanaged or jailbroken and rooted mobile devices are forcefully blocked from accessing the corporate data assets. Mobile enterprise end-to-end with the industry’s easiest-to-use are adequately protected with MDM. Zenprise’s Mobile Manager and has encourage enterprises by giving them the guts to accept BYOD and other corporate-owned mobile electronic transaction devices, by protecting sensitive corporate data, and the network from mobile threats, ensuring compliance with all regulatory and corporate policies in a simplified administrative process.

## 5. Conclusion

The main objective of this study was to inform IT, managers of organizational security function, the strategies to withstand most security threats, vulnerabilities, and risks associated with BYOD systems. What contributes to information insecurity has proven to be complex, dynamic and more of psychological in nature. Security measures need to be complex in order to handle the complex security threats. Organizations’ data confidentiality, integrity, and availability are becoming complex, dynamic and psychological. Perimeter defenses, control over devices, employee’s adherence to policies, control over policy enforcement, and enterprise definitions are no longer reliable as all security platforms are complex, dynamic and psychological. Attackers are personalizing their attacks. Security defenses must be personalized as well, with a holistic approach that expands beyond the technical security to include the environment, the technology, and the people There are differences in behavior intent towards implementation of security measures.

IT managers of BYOD security systems must put in place good policies coupled with good formulation and communication of same, information security policies intentions, principles, rules and guidelines which should be adhered that could avert all forms of security breaches.Employees and divisions within organizations that are responsible for transmitting and receiving confidential data need to know what is sensitive and what needs special protection. Ultimately, organizations are responsible for the security of their data regardless of the ownership of the device and therefore need to act responsibly with BYOD. It may not always be obvious, but data leakage could cost an organization in many ways. Organizations must provide privacy safeguards and select effective countermeasures to protect e-mails going outside the company, identify and mitigate against junk mail, phishing attacks, and malicious links and attachments in incoming e-mail. One of the biggest challenges in BYOD is to keep company's data secure and isolated from user's personal data.

There is the need to preserve user's privacy and at the same time maintain corporate information available and secure in the same device. Surely, it is possible to protect the company's data even if the data is located at the user's device by using the EMS leverages Azure RMS capabilities that provides data classification and protection with a BYOD Template created to restrict access to documents (Diogenes, 2014). Other security measures included the installation of antivirus software on employee personal devices so as to provide a kind of technical support while their devices are in use for business purposes. Other measures include having an acceptable and effective BYOD Policy that provides adequate guidance to employees using their own devices to process corporate and personal data. In general, more effective control access levels based on other device characteristics and policies could be achieved using a mobile device management solution (MDMS).

**References**

Arumugam, A., Yahya, D., Rozalina, K.,& Mohd, R. (2014).Usage of Learning Management System (Moodle) among Postgraduate Students: UTAUT Model. *Asian Social Science, 10*(14), 186-192.

Baskerville, R. (2011). Individual Information Systems as a Research Arena. *European Journal of Information Systems, 20* (2), 251-254.

Bell, E. E. (2017). A Narrative Inquiry: A Black Male Looking to Teach. *The Qualitative Report, 22*(4), 1137-1150.Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss4/12

Bhattacherjee, A., Limayem, M., & Cheung, C. M. K. (2012). User Switching of Information Technology: A Theoretical Synthesis And Empirical Test. Information & Management, 49, 327–333.

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., & Buckalew, L. (2013). BYOD: A global perspective, harnessing employee-led innovation. *Cisco IBSG Horizons*. Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf

Caine, V., Estefan, A., & Clandinin, D. J. (2013). A return to methodological commitment: Reflections on narrative inquiry. *Scandinavian Journal of Educational Research, 57*(6), 574-586. doi: 10.1080/00313831.2013.798833

CISCO. (2008). Data Leakage Worldwide: Common Risks and Mistakes Employees Make. Cisco white paper Public Information. http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf

Cristian, T. M., & Volkamer, M. (2013). Usable secure email communications: criteria andevaluation of existing approaches. *Information Management & Computer Security,21*(1), 41-52.

de Albuquerque, A. j., & dos Santos, E. (2015). Adoption of information security measures inpublic research institutes/adoç'o de medidas de segurança da informaç'o em institutosde pesquisa p'blicos. *Journal of Information Systems and Technology Management :JISTEM, 12*(2) 289-315. doi:10.4301/S1807-17752015000200006

Dernbecher, S., Beck, R., & Weber, S. (2013). Switch to Your Own to Work with the Known: An Empirical Study on Consumerization of IT. *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, Illinois, 15-17.

Diogenes, Y. (2014). Using EMS to Mitigate Data Leakage in BYOD Scenarios. Retrieved fromhttp://blogs.technet.com/b/yuridiogenes/archive/2014/11/26/using-ems-to-mitigate-data-leakage-in-byod-scenarios.aspx

Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks?*Technology Innovation Management Review, 3*(7), 6-11.

Durif-Bruckert, C., Roux, P., Morelle, M., Mignotte, H., Faure, C., &Moumjid-Ferdjaoui, N. (2014). Shared decision-making in medical encounters regarding breast cancer treatment: the contribution of methodological triangulation. *European Journal of Cancer Care, 24*(4), 461-472. doi:10.1111/ecc.12214

Dwivedi, Y., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., … Srivastava, S. C. (2015). Research on information systemsfailures and successes: Status update and future directions. *Information SystemsFrontiers, 17*(1), 143-157. doi:10.1007/s10796-014-9500-y

EYGM (2013). Bring your own device Security and risk considerations for your mobile device program. *Insights on governance, risk and compliance September 2013.* Retrieved fromhttp://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_ mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in informationsecurity risk management. *Information Management & Computer Security, 22*(5),430-410. doi:10.1108/IMCS-07-2013-0053

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments. *Journal of Information Privacy and Security, 11*, 38–5. doi: 10.1080/15536548.2015.1010985

Goode, S., & Lacey, D. (2011). Detecting complex account fraud in the enterprise: The roleof technical and non-technical controls. *Decision Support Systems, 50*(4), 702-714.

Greavu-Serban, V., & Serban, O. (2014). Social Engineering a General Approach.*Informatica Economica, 18*(2), 5-14. doi:10.12948/issn14531305/18.2.2014.01

Harris, J. G., Ives, B., & Junglas, I. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive, 11* (3), 99–112

Hartzog, W., & Stutzman, F. (2013). Obscurity by design. *Washington Law Review, 88*(2),385-418.

Hill, C., & Burrows, G. (2017). New voices: The usefulness of a narrative approach to social work research. *Qualitative Social Work: Research and Practice, 16*(2), 273-288. doi:10.1177/1473325017689966

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilitiesthrough situational crime prevention. *Security Journal, suppl. Special Issue: Securityin a digital world: Understanding, 26*(4), 383-402. doi:10.1057/sj.2013.25

Ho, L., Hsu, M., & Yen, T. (2015). Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL. *Information and Computer Security, 23*(2), 161-177. doi:10.1108/ics-04-2014-0026

Jahanian, R.,& Salehi, R. (2013). Organizational Culture. *International Journal of AcademicResearch in Progressive Education and Development, 2*(3), 84-96. doi:10.6007/IJARPED/v2-i3/82

Kumar, A. (2014). Bring Your Own Device (BYOD) Advantages and Disadvantages – 1Retrieved from http://www.thewindowsclub.com/bring-your-own-device-byod

Liu, S., & Kuhn, R. (2010). Data Loss Prevention. IT Pro. IEEE Computer Society. Retrieved from http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf

Loose, M., Weeger, A., & Gewald, H. (2013). BYOD – The Next Big Thing in Recruiting? Examining the Determinants of BYOD Service Adoption Behavior from the Perspective of Future Employees. Proceedings of the Nineteenth Americas Conference on Information Systems, 1-12

Magalhaes,R. M. (2011). Data Leakage Prevention. Retrieved fromhttp://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Data-Leakage-Prevention.html

Malcolm, P. M. (2017). Peer support in mental health: a narrative Review of its relevance to social work. *Egyptian Journal of Social Work, 4*(1). 19-40. doi:10.21608/ejsw.2017.8725

MobileIron (2012). Docs@Work: Data Loss Prevention and Secure Access for Mobile Content.http://www.mtechpro.com/2012/mconnect/october/dyncontent/ Docs@Work_White_Paper_20Aug2012.pdf

Montesino, R., & Fenz, S. (2011). Information Security Automation: How far can we go?

Nan, N. (2011) Capturing Bottom-Up Information Technology Use Processes: A Complex Adaptive Systems Model, *MIS Quarterly, 35* (2), 505–532.

Okesola, J. O., & Grobler, M. (2014). Developing a secured social networking site usinginformation security awareness techniques. *South African Journal of InformationManagement, 16*(1), 1-6. doi:10.4102/sajim.v16i1.607

Oye, N. D., AIahad, N., &Abrahim, N. (2014). The history of UTAUT model and its impact on ICT acceptance and usage by academicians. *Education and Information Technologies. 19*(1), 251-270.

Pfleeger, S.L., Predd, J.B., Hunker, J.,& Bulford, C. (2010). Insiders Behaving Badly:Addressing Bad Actors and Their Actions. *Information Forensics and Security, IEEETransactions on, 5*(1), 169-179. doi:10.1109/tifs.2009.2039591.

Privizzini, A. (2017).The Child Attachment Interview: A Narrative Review. *Frontiers in Psychology, 8*(1), doi:10.3389/fpsyg.2017.00384

Purohit, B., & Singh, P. P. (2013). Data leakage analysis on cloud computing. International *Journal of Engineering Research and Applications (IJERA), 3*(3),1311-1316

Rutherford, J. S. (2017). Monitoring teamwork: a narrative review. *Anaesthesia, 72*(1), 84-94. doi:10.1111/anae.13744

Scarnato, J. M. (2017). The value of digital video data for qualitative social work research: A narrative review. Qualitative Social Work: Research and Practice, doi:10.1177/1473325017735885

Shabtai, A., Elovici, Y., & Rokach, L. (2012). A Survey of Data Leakage Detection andPrevention *Solutions, 20*(3), 23-44. doi:10.1007/978-1-4614-2053-8_2

Shehata, G. M. (2015). Leveraging organizational performance via knowledge managementsystems platforms in emerging economies: Evidence from the Egyptian Information andCommunication Technology (ICT) industry. *VINE, 45*(2), 278-239. doi:10.1108/vine-06-2014-0045

Siciliano, R. (2014). Employees Are the Greatest Risk to Your Company's Security Network. Retrieved from: https://www.linkedin.com/pulse/20140219043628-1778940-employees-are-the-greatest-risk-to-your-company-s-security-network

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296– 302. doi:10.1016/j.im.2011.07.002

Stewart, G., & Lacey, D. (2012),"Death by a thousand facts", *Information Management &Computer Security, 20*(1), 29-38. doi:10.1108/09685221211219182

Symantec (2015). Symantec Data Loss Prevention. Data Leak Prevention. Retrieved from http://www.symantec.com/data-leak-prevention/

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *Management Information Systems Quarterly, 27*(3), 1-12.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: a framework & its analysis. *Computers & Security*. doi:10.1016/j.cose.2015.06.011.

ZENPRISE_DLP (n.d.). Mobile DLP (Data Leakage Prevention). Retrieved February 22, 2015 from http://www.ndm.net/mobile/Zenprise/mobile-dlp

ZENPRISE_MDM (n.d.). What is Mobile Device Management (MDM)' Retrieved February 22, 2015 from http://www.ndm.net/mobile/Zenprise/mdm

Zhou, T., Lu, Y., &Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption.*Computers in Human Behavior, 26*(4), 760-767.