Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

BYOD adoption concerns in the South African financial institution sector

Andreas Gustav
University of Cape Town, andreas.gustav@alumni.uct.ac.za

Salah Kabanda
University of Cape Town, salah.kabanda@uct.ac.za

18. BYOD adoption concerns in the South African financial institution sector

Andreas Gustav
University of Cape Town
andreas.gustav@alumni.uct.ac.za

Salah Kabanda
University of Cape Town
salah.kabanda@uct.ac.za

Abstract

Bring Your Own Device (BYOD) is an emerging trend and practice that is growing in use in many organizations. There is however very limited literature on BYOD in the context of financial institutions from a developing country perspective. The dearth of such studies is problematic because financial institutions deal with a lot of sensitive and confidential information and therefore their adoption of BYOD could be detrimental to their practice. This study contributes to this gap in literature by providing empirical observation that show how technological and contextual factors affect financial institutions adoption of BYOD. Following a qualitative approach, and using semi structured interviews as a source of data collection; the findings show that cost, complexity, a culture of innovation, and top management support were factors that were perceived as enablers of BYOD. South African organizations in the financial services use BYOD to help add value to their work as opposed to it being a cost saving necessity. However, the continuous changes in government regulation regarding the use of data; and the lack of conducive ICT infrastructure were deemed as hindrances to BYOD. As a result of the changing regulations and the lack of knowhow on implementation of these regulations, most organizations failed to formalize their BYOD strategies.

Keywords

Developing countries, Bring Your Own Device (BYOD), Financial Institutions.

1. Introduction

The increase in the use of personal mobile devices in the workplace has given rise to a new phenomenon called Bring your own device (BYOD) which affords employees the ability to use their personal devices to access their organizational resources in order to perform everyday work tasks (James & Griffiths, 2012; Putri & Hovav, 2014; Walker-Osborn, Mann, & Mann, 2013). Evidences specifically from the developed economies show how organizations are greatly benefiting from BYOD adoption (Lee et al, 2013). BYOD allows organizations to reduce costs on mobile computing device purchases and expenses as they pass the responsibility of purchase onto the employee potentially saving the organization money in operational expenses (Lee et al., 2013; Smith & Forman, 2014). Smith & Forman (2014) found that employee's satisfaction and productivity increases when they are allowed to bring and use computing devices that they are comfortable working with. Despite these benefits, a significant number of studies have shown that BYOD raises a number of risks and challenges for organizations – specifically security concerns that are inevitable because the ability to access company networks on private devices

makes the organization susceptible to data leaks, malware attacks or data loss (Putri & Hovav, 2014). In addition, BYOD could lead to loss of devices containing company sensitive information (Lebek, Degirmenci, & Breitner, 2013; Morrow, 2012). These challenges however, have not deterred organizations from embracing BYOD.

Although BYOD as a trend is more prevalent in the developed economies; Smith et al. (2011) noted that the rapid increase in mobile device usage in the developing countries is a positive move towards readiness for BYOD adoption. This increase in usage has in turn driven down the prices of smartphones and their wide usage is predicted to increase in the near future (Aker, 2010; Bidwell et al., 2013). As a result, BYOD adoption in developing countries is slowly becoming a reality, although the empirical evidence is still scanty – specifically from the financial institutions realm. Most studies that investigate the BYOD phenomena have not been in the financial industry – a sector with a great amount of personal and private information which needs to be properly monitored and safe guarded (Shepherdson, 2013). These institutions are usually at the fore-front of maintaining a high data and corporate integrity. The lack of empirical evidence in this area renders decision makers of financial institutions a disadvantaged when it comes to BYOD. Therefore this study investigates the BYOD phenomenon from a financial institutions perspective within the South African context. Specifically, the study seeks to identify what factors are important to consider prior to adopting BYOD in the financial sector. The rest of the paper is structured as follows: Section 2 presents related work in the field of BYOD. Section 3 discusses the methodology. Findings are presented in section 4. The discussion of the findings is done in section 5. Section 6 concludes the paper.

2. Related work

2.1 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) is a phenomena that refers to employees bringing their personally owned mobile devices (laptops, tablet or smartphone) to work to do their work tasks (Putri & Hovav, 2014). A personally owned device is usually any mobile device used in the workplace and is owned by the employee and not the organization (Smith & Forman, 2014). Employees that are afforded the liberty to use their own devices for work purposes, gain from the convenience of being able to work in geographically diverse locations with devices of their choice and comfort. The adoption of BYOD in organizations give rise to increased job satisfaction, increased staff productivity, lower ICT costs and attractiveness to potential qualified employees (Astani et al., 2014; Lee et al., 2013; Smith & Forman, 2014). The use of personal devices in organizations means that employers do not need to purchase ICT devices for their employees (Smith & Forman, 2014). This saves the organization the cost of buying ICT devices such as laptops, tablets and smartphones for their employees (Lee et al., 2013). Caldwell (2012) also found that a reduced investment in ICT devices helps to reallocate the organizational budget to other expenses.

Although BYOD bring many benefits to organizations, it also introduces many risks. These risks may include security issues through malware attacks, privacy concerns through data leaks, loss of the devices, cost of device management software and disparities in the different available devices (Lebek et al., 2013; Putri & Hovav, 2014; Berghaus & Back, 2014). Although companies spend large sums of money to ensure their data is not leaked or compromised (Hunt, 2012), employees are unlikely to have similar security measures on their personal devices. The problem

management is faced with is trying to find the best way to allow employees access all their data and resources while keeping that data safe and secure (Smith & Forman 2014; Hunt, 2012). Also, employees may be dismissed or choose to leave an organization at some point and the company data on their personal device may be at risk of loss or exposure (Friedman & Hoffman, 2008; Morrow, 2012). Another challenge is the cost of managing the devices. In as much as BYOD could save organizations money, it also increases the cost for device management software.

2.2 Theoretical approach

This study uses the technological, organizational and environmental framework (TOE) framework to explore factors to consider prior to adopting BYOD in the financial sector. TOE describes not only the process by which a firm adopts and implements technological innovations (Ortbach et al, 2014); but also how technological, organizational and contextual factors impact adoption. The technological context describes both the internal and external technologies relevant to the organisation, the practises, processes and the equipment used while considering other technological features (Oliveira & Martins, 2011). These technologies include both those that are already used within the organisation as well as those that are available in the marketplace but haven't currently been utilized by the organisation (Baker, 2012). The organisation context refers to the measures about the organisation such as the scope, size, managerial structure, demographics, and its perceptions with regard to innovation and also how ready the organisation is in terms of resources such as finance, technology and expertise to adopt and use an innovation (Oliveira & Martins, 2011). For example, organisations that are small in size tend to lag behind their larger counterparts because of the scarcity of resources needed to initiate the deployment of new innovations required for the initial set-up and sustenance of such an innovation (Teo et al., 2009). How an organization perceives an innovation can also affect adoption intentions. Management's failure to perceive the benefits can ultimately lead to underestimating the impact of the innovation and prefer to be followers rather than leaders in the adoption process (Kaynak et al., 2005, 638). Benefits tend not to be seen when the costs tend to be perceived higher or when the innovation is perceived as being complex. However, if management perceive the innovation to be compatible with the organisation's strategy it can be adopted.

The environmental construct assess the external factors of the organization such as 'government laws and regulations, social structure, national policies, technical change and the natural environment that directly impact the companies' towards its intention to adopt an innovation. Molla and Licker (2005, 878) define external factors to include 'market forces, the government, and other supporting industries'. To adopt an innovation, organizations need to perceive that the external environment is favourable. They will have to assess the willingness and readiness of both consumers and trading partners to partake in the adoption and use of the innovation. Organizations need to assess the social readiness to adopt the innovation; and the role of the government in establishing a conducive environment for the use of the innovation.

3 Methodology

The study is interpretive in nature, and data was collected using semi structured interviews. The interviews were largely open-ended and the participants were afforded the liberty to discuss their options and choices accordingly. The interview questions were informed by the literature review from the onset; however the researcher continuously added or removed questions as more in-sights were gained into the BYOD phenomenon. The sample of respondents was identified and

chosen based on their role as key players in the South African financial services industry. The sample frame consisted of the main organizations in the South African financial services industry. The sample included four commercial banks and one insurance company. Table 1, shows the four banks sampled and the one insurance company. The banks A-D, were very similar in nature as they delivered primarily the same products and services to a competing target market. The commercial banks were essentially institutions which offered basic banking services such as bank account hosting, investment facilities, short home loans and vehicle and asset financing. The insurance company being one of the biggest in Africa, covered clients on health insurance, life insurance, car and natural disaster insurance. Each of the participating institutions had two members of their organization interviewed. The respondents interviewed were all on management level because the decision to adopt BYOD would lie with management as opposed to operational staff. Participants were initially contact via email, with personalized letter attached. An appointment date was then set up that suited both the researcher and the respondent.

Financial Institution Code	Respondent Code	Role in organization
Bank A	Respondent A1	Branch Manager
	Respondent A2	Head: Banking Services
Bank B	Respondent B1	Manager: Home loans
	Respondent B2	Branch Manager
Bank C	Respondent C1	Manager: Customer Services
Bank D	Respondent D1	Manager: Customer Services
Insurance Company E	Respondent E1	Head: IT
	Respondent E2	Head: HR

Table 1: Sample of respondents

The researcher conducted eight interviews in total during the study. All of the interviews were Cape Town based and as such they were all face-to-face interviews. Only two of the eight inter-views were not recorded as participants were uncomfortable with recording. In the instance of no recording, note taking and observation were used as means of data collection. It should be noted that recording was not perceived as an option because of the confidentiality purposes attached to such institutions. After each inter-view, immediate transcription took place so as to not lose the essence of the social production of the interview. After transcription, the interview reports were sent back to the respondents for confirmation purposes. In this manner, triangulation was made possible and also assist in ensuring that data that was missed during the interview was included. This proved valuable for the interview sessions with respondents who did not want to be recorded. Data analysis followed a thematic approach which commenced by reading each transcribed interview with the intention of familiarizing oneself with the script. Then, the researchers reread the each interview multiple times with the purpose of immersing oneself in the interview setting so as to relive the experience once again. In each of these exercises, notes were made that appeared to be important to that specific interview. These notes were analyzed to identify repetitive occurrence of concepts/terms across the entire data set (across the 8 interviews), and in so doing arriving at themes that represent the major findings.

4 Findings

The findings from the analysis are categorized into three main themes: technology, organization and environment as discussed in the subsections that follow.

4.1 Technology

4.1.1 Cost

The findings show that respondents were not aware of but highly interested in the cost implications related to the implementation of a BYOD strategy in their organizations. Although BYOD had been adopted in some organization, the full cost implication had not been determined and this was perceived as a challenge because according to RespondentA1: "*BYOD cost money because we will have to insure the devices and also monitor data usage*". Similar remarks were expressed by other participants. Respondent D2 expressed the fear of implementing a costly BYOD monitoring system that will strain time and human capital: "*a monitoring system is a must, considering the nature of our operations but remember this will require time and effort. Will we need to add more staff? Train the current staff? Increase the duties of current staff which may mean increasing their packages, all these need to be considered from a management perspective…*" Additional costs that were implicated were those related to varying devices used by employees which may increase costs as respondent C1 notes: *"...it's very tricky because not everybody uses the same type of phone. Some use Samsung, other Apple and others Sony or whatever and these each have different sizes, resolutions that need to be considered. It's not easy at all*". Although all respondents indicated that the full cost implication had not been determined for adopting BYOD, they did state that prior to implementation of any project; "*IT teams are required to provide detailed perceived benefits analysis using statistics and financial projections. Also, IT projects have strict timelines and are expected to display success stories of similar implementations or demonstrate the probability of success*" (respondent C2). The implications was that a BYOD implementation strategy was not supported if it was perceived to be financially burdensome on the organization because *"…technology is something we are proud to leverage off to gain value and BYOD is no different*" (Respondent B1). In addition, for most organization, implementation was highly driven by success rates of similar projects in organizations that are within the same industry.

4.1.2 Technology Complexity

All respondents in this study did not find the implementation of BYOD as a complex phenomenon for their organization. Respondent A2 elaborates: *"…it's important to look at how complex an IT project is. Complexity speaks about time, human effort and resource allocation. It needs to be considered…in the BYOD debate complexity is not so important because we are looking at people using their own phone and tablets. Sounds easy"*. This was reinforced by respondent C1 who added "*Complexity? I think BYOD is quite straight forward in comparison to other IT projects"*. What was deemed difficult to establish was the maintenance of privacy and security concerns as respondent B2 explains: *"…the only real concern with complexity is the split between what you can and cannot monitor at an organizational level. That's it*". This is further shared by respondent C1 who added *"Complexity? I think BYOD is quite straight forward in comparison to other IT projects".* The implications is therefore that complexity was not perceived as a strong factor for BYOD implementation in the financial industry although cautions should be given to how an organization plans to address privacy and security concerns which could prove to be a daunting task.

4.1.3 Security and privacy

The most consistently highlighted factor perceived to be important to consider by all respondents, prior to implementing BYOD, was the issue of security. This was attributed to the very nature of the industry which has a great amount of personal and private information which needs to be properly monitored and safe guarded. Respondent C1 elaborates extensively: *"… we are risking our organizational integrity with this technology. It is scary and we need to be very care of how we handle it… I really think in our industry the client comes first and as a consequence the protection of all and any data they have entrusted us with is also our number one priority.*" The financial services industry boasts a great deal of customer centric operations where personal and confidential information is put in the hands of financial companies and as such *"we need to ensure we safeguard such information especially in light of BYOD's practice of using personal devices. The data on our systems was continually threatened by hackers… hackers will not stop. They keep trying and finding new ways to penetrate our data. We are equally forced to constantly revisit our security protocols. We have already been victim to SQL injection and denial of service attacks in recent months"* (Respondent C2).

Respondent D1 was more vocal on privacy concerns indicating that BYOD threatened the privacy of an employee where the organization decides to install monitoring application on the device: *"It is difficult to separate what can and cannot be monitored on a mobile device. We don't want a case where an employee's private message or phone calls can be monitored by the company".* The eminent fear of losing control over their data was evident across all organizations because according to respondent D1: *"We are in a space where technology can actually risk our entire organization's practice. Security is very imperative in the BYOD adoption debate and we surely don't want to lose customers simply because they don't trust the security of our systems to keep their information confidential. This BYOD thing exposes us to such threats and it must therefore be well thought of".* As a result of these concerns, organizations such as E perceived "*BYOD as a platform for us to put into place stringent security measures to ensure the technology adds rather than detracts value from the business"* (Respondent E1). Most respondents suggested an intelligent monitoring application be installed in all registered employee devices so that the organization still maintains control of important information. The implementation of such an application is important because *"…then we can see if and when an employee shares information they are not supposed to… we are able to track the whole phone's major activities. We provided the devices ourselves and thus this was easy but employees have still complained about needing some privacy and we now are working on a newer iteration that will address the privacy issue"* (Respondent D2). The implications of these findings point to the fact that institutions of a financial nature should always strive to safeguard and improve the quality of their data security in the wake of BYOD because BYOD is no different and companies should *"… we need to always think very carefully about what you are exposing and how to avoid such exposure"* (Respondent A1). Thus security and privacy of BYOD as a technology in a financial company is of utmost importance when considering BYOD adoption.

4.2 Organization

4.2.1 Top Management Support

The findings show that for the BYOD strategy to be successfully implemented and address privacy and security concerns adequately; top management support was essential. However,

respondents called for the need to show management the *"the value of what you are proposing for them to buy into it"* (Respondent B1); and the *"serious security concerns for the bank"* (respondent D2). These were highlighted so that management can have a say especially if budgets need to be adjusted to take into account security and privacy measures. There were concerns that top management tend to leave technology important matters to the IT department and fail to participate in the development of BYOD strategy that is safe for the organizations. *"Imagine management that sits in your development meetings or iterations to provide insights and advice. It's the ideal situation but sadly not the case often. You can have management that is supportive of innovation whilst talking about it, but not in providing the financial support for it. This is inadequate."* (Respondent B2). Top management was perceived to possess the power to assign budgets that can address BYOD security risks and technical costs because *"… at our level, we can suggest all we want but the big bosses (top management) always have the final say"* (respondent D1). The consensus was that top management was important for technology driven projects to thrive as opposed to leaving these projects to be driven by IT departments alone because according to respondent E2 *"…at the top level, a lot of things are considered - looking at how something like BYOD will affect the greater spectrum of the company. They look at HR, employees, IT, finances and possible change in strategy".* The implications of these findings point to the fact that top management that is supportive of new IT practices such as BYOD was one of the factors contributing to a successful BYOD implementation, as respondent E1 states: *"… the chances of success for BYOD increases substantially if a very supportive top management structure is behind it".*

4.2.2 Organizational Culture

Most respondents indicated they had already embraced a culture of innovation that acknowledges new practices of using technology. Respondent A2 states: "*I definitely think we are one of the most fluid and flexible banks out there. We welcome change and alter our ways of doing things accordingly"*. Organization A boasted of their mobile banking application which they were *"constantly innovating and finding easier ways of doing things"* (respondent A2). Organization C had *"embraced the mobile wave. We were a bit late to be honest but I think we are there now…one can sense the culture of innovation in the organization since everyone uses our products themselves before selling to our clients*" (respondent C1). Other organizations such as organization B and D were already allowing employees access to company emails and intranet on privately owned devices. They however did indicate that this was not formalized regardless how embracing they are of technology and innovation. The findings imply that organizational culture was an important factor in the adoption of BYOD. The financial institutions that are very welcoming of technological changes, innovation and new ideas are more likely to invest in BYOD than those who do not.

4.3 Environment

4.3.1 Government Regulations and Compliance

The need for constant government compliance was perceived by all respondent as a challenge. This was partly due to the constant change in laws; and lack of know-how of these laws. Respondent C1 clarifies: *"…everything we do needs to be within the expectation of the law. It's very challenging because BYOD is new and it still has to be learnt in terms of its full implications… and the new laws such as POPI that are there also have to be understood in relation to BYOD. We are not knowledgeable here".* POPI, the Protection of Personal

Information act ensures that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise gathered personal information in any way. With this new act in mind, respondent A2 states: *"with BYOD and this new law…it is very tricky I tell you. POPI clearly states that one's information and privacy should be protected at all times. This is difficult to guarantee with the use of BYOD*". Respondent C2 agrees indicating that *"the law requires us to have consent from the customer before we use their information for whatever reason and we can make them sign something but how do we ensure BYOD does not place us in a compromising situation".* There was consistent agreement that the implications of POPI on BYOD was not yet known and *"this needs to be investigated lest we find ourselves not being compliant unknowingly… we have a duty, not only to our customers but importantly to the state to ensure all our operations are as the book prescribes"* (respondent E1). The findings call for the need to provide the financial industry with awareness and education of the policies and laws such as POPI that have recently been enacted and that have a consequence on their operations. The lack of commitment from top management to formalize BYOD could be associated with their lack of know-how regarding the full implications of these laws.

4.3.2 Industry Competitors

The findings show that all organizations regarded competition as an important element that cultivated new product development and innovation; and as such relevant for any innovation adoption such as BYOD. Respondent B2 highlighted the importance of competition in the financial services industry: *"Competition is healthy…the necessity of observing and learning from the success and failure stories of competitors is of utmost importance to us*". Financial institutions therefore perceived competition as an opportunity to not only be the leader in the market and gain competitive advantage over their industry peers (respondent B2, C2); but also as a lesson towards understanding why some organizations fail, for example during the implementation of a project. Respondent D1 raised the concern of a company implementing a common invention and failing at it because of an organizational misfit: *"The truth is some technologies or innovations are specific to particular organizations. Because it worked for Bank X doesn't necessarily mean it will work for bank Y. Careful consideration needs to be made*". Respondent E2 agrees as he pointed out that his organization once had a failed IT project because it didn't meet their business requirements: *"… we were simply too keen to jump onto the bandwagon without assessing our business requirements first. It was a failed project that we learned a lot from".* The findings show that most respondents agree that the activities of industry competitors should be taken into account when making adoption decisions. However, other respondents explained the need to be cautious of what activities to emulate especially if they do not have an organizational or operational fit with one's company.

4.3.3 National ICT Infrastructure

All respondents identified the national ICT infrastructure as not being conducive for the adoption of new innovation and practices, partly because of the costs associated with it (respondent C2); and partly because of the "*increase in the use of mobile devices, especially in the developing countries such as South Africa which puts strain on the national infra-structure that is expected to host and provide an a error-free coverage and support"* (Respondent D2). Respondent B1 explained: "*We are improving but we still have a long way to go. Countries that have successful BYOD adoption are in Europe and North America because their infra-structure and bandwidth*

is second to none". BYOD adoption and the quality of BYOD activities was associated with better bandwidth and much fast Internet connections. However according to respondent C2, "*an increase in speed comes at a cost. We are always weary of the cost attached to faster Internet and to aid BYOD it will also have to be at a cost that needs to be motivated for"*. Several solutions have been proposed for addressing this challenge. One of them is the use of Asymmetric Digital Subscriber Lines (ADSL) which is seen as a way of solving band-width problems at minimum expenses. However, respondent D1 raised reliability concerns: *"ADSL is relatively affordable but it's physical and often has high downtime due to cable theft and so forth".* Another solution was to put pressure on the service providers. For example Respondent E2 challenged Telkom, a wireline and wireless telecommunications provider in South Africa, *"to improve the reliability of their infrastructure…it really needs to get a grip of the ICT field before it's too late. They run almost everything and we continue to depend on their highly unreliable services".* The final solution comes from the financial industry players who have embarked on developing their own networking to assist their systems: *"We recently announced our plan to launch our own mobile network. This is more for us to have a network infrastructure that we can predict and control such that our secondary networks and servers get no downtime"* (Respondent A1). These findings show that bandwidth and Internet accessibility and reliability were considered as factors that challenged the use of BYOD practices and as such impacting the decision to adopt in the South African financial industry.

5 Discussion

This study identifies three factors as important for organization in the financial sector to consider. These include technology, organization and environmental factors. The factors under the technology constructs include the costs, complexity and privacy and security concerns related to the adoption and implementation of BYOD. Most organizations perceive cost associated with BYOD as one of the deterrent factors to BYOD. However they found that BYOD is not complex to adopt. Similar findings are reported by Chountalas and Karagiorgos (2015) who found that BYOD's use is non-complex and therefore was more of an enabler than a hindrance to adoption. However, the findings in this study show that complexity was an issue when privacy and security concerns had to be addressed. Privacy and security were factors that resonance throughout the data corpus due to the sensitive information that the institutions hold. The implementation of these privacy and security solution was perceived to be complex because of the diverse products which employees use.

Consistent across all organization was the fact that investment into BYOD required commitment from top management to provide the financial and political will to specifically address privacy and security concerns. In addition, a thorough readdress of environmental variables, specifically government regulations, industry competition and national ICT infrastructure, was necessary prior to BYOD adoption and implementation. Respondents were more vocal on the impact of government regulation because *"…everything we do needs to be within the expectation of the law. It's very challenging because BYOD is new and it still has to be learnt in terms of its full implications".* As such compliance to government and industrial regulations, as well as the challenges of the national ICT infrastructure were perceived as hindrances to BYOD adoption. These findings however deviate from Akin-Adetoro and Kabanda (2015) who state that contextual factors of supporting industry, government readiness and market forces were not as important as organizational factors when it came to adoption. This is not surprising because the

industry context in this study and the size of the organizations defer immensely with those of Akin-Adetoro and Kabanda (2015) who investigated BYOD in SMEs – organizations that tend to have resource constraints in comparison to financial institutions such as Banks used as cases in this study. Also the findings in this study are reflective of financial institutions in the Western Cape of South Africa, a very advanced area in the Sub Saharan region of the African continent in terms of infrastructure and resources. Although organizations in this study perceived themselves as being adequately resourced; they were unable to formalize a BYOD strategy despite having adopted BYOD. The most prominent reason was associated with external factors such as government regulations and the lack of a conducive ICT infrastructure. Similar findings have been reported in other studies. However, these findings have been consistently applied to SMEs (Harris and Patten 2015; Kurpjuhn 2015; Kabanda and Brown, 2014), and other sectors such as the education industry (French et al 2015; Rahat 2014) that do not have a great amount of sensitive personal and private information which needs to be properly monitored and safe guarded as financial institutions.

6 Conclusion

The purpose of this study was to investigate the BYOD phenomenon from a financial institutions perspective within the South African context. Specifically, the study goal was to identify factors perceived to be important prior to adopting BYOD in the financial sector. Following a qualitative interview approach and thematic analysis, the findings revealed that financial companies adopt BYOD mainly for convenience as it is seen as a value adding practice to their daily tasks. However, this adoption was not formalized. The factors perceived to be important prior to adopting BYOD in the financial sector were categories in three main groupings for ease of representation: Technology, organization and environment. The factors perceived to be negatively associated with BYOD adoption included the cost and the security and privacy concerns associated with implementation. Complexity of BYOD was not perceived as a factor to be concerned with. Organizations in the financial sector perceived top management support and an organizational culture that supports innovation as crucial in the development and implementation of a successful BYOD strategy. Matters relating to technology strategy, specifically on issues that raised IT concerns such as security and privacy, were perceived to be top management priority and should be driven and supported by them, instead of being given to the IT department to drive them. However the findings show that for the financial sector to be successful in its adoption of new practices, such as BYOD, there needs to be constant awareness and education about government regulations and their implications on new innovation and ways of doing things. There was resistance to formalize BYOD due to the lack of know-how and awareness of the consequence of the new POPI act. Although organizations welcomed competition within the financial sector they noted that the lack of a conducive national ICT infrastructure was a barrier to most of the organization's implementation of new innovative practices which required low bandwidth and high Internet accessibility that is reliable and less cost effective for developing countries.

Several limitations to the study are noted. Firstly although TOE was used to interpret the data, a more grounded theory for qualitative studies such as structuration theory would have provided richer understanding of the phenomenon, specifically on explaining the interaction between employees and mobile devices. Secondly, the unit of analysis are Banks, of which some had not adopted BYOD. For an in-depth interpretive study, it would have been valuable if the eight

respondents were from the same organization that has already adopted BYOD. In so doing, the finings would have paved the way for future investigation into for example specific security threats peculiar to financial institutions.

References

Adedolapo A, and S. Kabanda (2015). "Contextualizing BYOD in SMEs in developing countries." In Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists, p. 3. ACM, 2015.

Aker, J. C., and I. M. Mbiti (2010). "Mobile phones and economic development in Africa". Journal of Economic Perspectives, (3)24, pp.207-232.

Astani, M., Ready, K., and M. Tessema, (2013). "BYOD issues and strategies in organizations". Issues in Information Systems, (2)14, pp. 195-201.

Baker T. (2013) "What you think about BYOD", SC Magazine: For IT Security Professionals, pp. 32-33

Berghaus, S., and A. Back. (2014) "Adoption of Mobile Business Solutions and its Impact on Organizational Stakeholders." (2014).

Bidwell, N. J., Siya, M., Marsden, G., Tucker, W. D., Tshemese, M., Gaven, N, and K. A. Eglinton, (2013). "Walking and the social life of solar charging in rural Africa". ACM Transactions on Computer-Human Interaction (TOCHI), (4)20, pp.1-33.

Caldwell T. (2012) "Prepare to fail: creating an incident management plan" Computer Fraud & Security, (11), pp 10-15

Chen, H., J. Li., T. Hoang., and X. Lou (2013). Security challenges of BYOD: a security education, training and awareness perspective.

Chountalas, P., and A. Karagiorgos (2015, March). Bring Your Own Device Philosophy from the User's Perspective: An Empirical Investigation. In Proceedings of the 2nd HOBA International Conference (1), pp. 1-12.

Emery, S. (2012). Factors for consideration when developing a bring your own device (BYOD) strategy in higher education (Doctoral dissertation, California College of the Arts).

French, Aaron, Chengqi Guo, Mark Schmidt, and J. P. Shim. "An Exploratory Study on BYOD in Class: Opportunities and Concerns." (2015).

Friedman, Jon, and Daniel V. Hoffman. (2008) "Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defences." Information, knowledge, systems management (1-2)7, pp. 159-180.

Harris, M. A., and K.P. Patten. (2015). "Mobile Device Security issues within the US Disadvantaged Business Enterprise Program." Journal Of Information Technology Management, (1)26, pp.46.

Hunt, J. (2012) "BYOD Policy–What Businesses Need to Consider." Credit Control (5)33, pp. 6.

James, P., and D. Griffiths, (2012). "The mobile execution environment: A secure and non-intrusive approach to implement a bring you own device policy for laptops". Australian Information Security Management Conference, (1)18, pp.82-89.

Kabanda, S. and I. Brown (2014). "Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries–The Case of Tanzania." ACIS, 2014.

Kaynak, E., Tatoglu, E., and Kula, V. (2005). An analysis of the factors affecting the adoption of electronic commerce by SMEs: Evidence from an emerging market. International Marketing Review, 22(6), 623-640.

Kurpjuhn, T(2015). "The SME security challenge." Computer Fraud & Security 2015, (3), pp. 5-7.

Lebek, B., Degirmenci, K., and M. H. Breitner (2013). “Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices”. Nineteenth Americas Conference on Information Systems, (1)19, 13-35.

Leclercq-Vandelannoitte, A. (2015). Managing BYOD: how do organizations incorporate user-driven IT innovations?. Information Technology & People, (1) 28, pp.2-33.

Lee, J., Crossler, R., and M. Warkentin (2013). “Implications of monitoring mechanisms on bring your own device (BYOD) adoption”. Thirty Fourth International Conference on Information Systems, (3)34, pp.2-6.

Molla, A. and Licker, P.S. (2005). E-Commerce adoption in developing countries: A model and instrument. Information & Management, 42, 877–899.

Morrow, B. (2012). “BYOD security challenges: Control and protect your most sensitive data”. Network Security, (12), pp.5-8.

Moschella, D., D. Neal., P. Opperman., and J. Taylor (2004, June). The ‘consumerization’of information technology. In Leading Edge Forum.

Oliveira, T., and Martins, M. (2011). Literature Review of Information Technology Adoption Models at Firm Level. Electronic Journal of Information Systems Evaluation, 14(1), 110–121.

Ortbach, K., Brockmann, T., and Stieglitz, S. (2014). Drivers for the Adoption of Mobile Device Management in Organizations. Twenty Second European Conference on Information Systems, Tel Aviv

Putri, F. F., and A. Hovav, (2014). “Employees´ compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory”. European Conference on Information Systems, (5) 22.

Rahat A. (2014) "Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges." International Journal of Emerging Trends & Technology in Computer Science, (1)3, pp. 233-236.

Shepherdson, M. (2013). “BYOD – the biometric implications”. Biometric Technology Today, (4)2013, pp.5-7.

Smith, K. J., and S. Forman (2014). “Bring your own Device—Challenges and solutions for the mobile workplace”. Employment Relations Today, (4)40, pp.67-73.

Smith, M. L., R. Spence, and A. T Rashid. (2011). “Mobile Phones and Expanding Human Capabilities,” Information Technologies & International Development (7:3), pp 77-88.

Teo T.S.H., Lin S., and Lai K. (2009). Adopters and non-adopters of e-procurement in Singapore: An empirical study. Omega, 37, 972-987.

Walker-Osborn, C., S. Mann, and V. Mann, (2013). “To BYOD or… not to BYOD”. IT NOW, (1)55, 38-39.