Individual traits that determine the Bring Your Own Device information security culture: A case study of the banking sector in Zimbabwe

Alfred Musarurwa[1], Stephen Flowerday[2], and Liezel Cilliers[3]
Department of Information Systems
University of Fort Hare
East London, South Africa
Email:amusarurwa@hotmail.com, sflowerday@ufh.ac.za, lcilliers@ufh.ac.za

Abstract

Information security in the banking sector is heavily controlled as banks store and manage their clients' private information. Information security has always been the responsibility of the information technology (IT) department in organisations. The Bring Your Own Device (BYOD) phenomenon has enabled employees to connect to the organisational network with their own devices. However, the IT department cannot easily prescribe information security measures for these devices, compelling organisations to entrust the security of the bank's information assets with the employee who inadvertently becomes the unintended administrator of information security on their private devices. While technology solutions have been developed for BYOD dilemmas, the human aspect that will implement and comply with these solutions has been neglected. The purpose for this paper is to investigate the individual traits of banking employees that will contribute to the BYOD information security culture. The banking sector in Zimbabwe is the context within which the study was conducted. The paper makes use of a literature review to inductively extract individual traits that will contribute to the BYOD information security culture. The traits were tested making use of a survey distributed among 270employees for a bank in Zimbabwe. The response rate was recorded as 87%. Analysis of the survey results was done leading to the conclusion that employee individual traits are significant for the BYOD information security culture (BYOD IS).The paper identified the individual traits of attitude, knowledge and habit to be key in improving the information security culture for the BYOD unintended administrator and recommends that the management of the bank should consider these when implementing BYOD initiatives for employees.

Introduction

The Bring Your Own Device (BYOD)phenomena has established itself as a growing and dynamic business trend that is also finding its way into the banking sector(Ginovsky, 2012).According to Lebek, Degirmenci, and Breitner (2013), BYOD enables employees to use their private mobile devices to access and manage organisational data from anywhere at any time. The massive influx of the smartphones and the exponential growth in Internet bandwidth has catalyzed the growth BYOD usage in organisations(Musarurwa & Jazri, 2015). Eschelbeck and Schwartzberg(2012) caution that BYOD is becoming the rule rather than the exception in today's workplace, leaving organisations with no other choice than to embrace the technology. The BYOD phenomenon is also redesigning the way businesses largely operate due to an increase in the number of organisations opening their networks and data to ubiquitous devices(Gens, Levitas, & Sega, 2011). Findings by Son and Jai-Yeol(2011) suggest that over half a million IS breaches occurring in organisations emanated from employee personal devices that have gained access into the network. Organisations are at different maturity levels in implementing IS, and this is why Zahadat, Blessner, Blackburn, and Olson (2015) emphasize that best practices for establishing BYOD IS policies are not yet established.

The BYOD phenomenon has also introduced new challenges to existing information management practices in organisations. Abramson (2014) recommends that organisations must invest in improving the current information security (IS) management processes if they want their network to be secure. This is especially important in the banking sector which is heavily controlled in order to protect clients' private and confidential financial information (Lund &Silva, 2015). Whilst banks have limited control of BYOD devices and the bank information these devices contain and have access to, the security of the information contained on these devices remains the bank's key concern. As employees use their private devices, Liu (2014) recommends that IS for BYOD must become every employee's responsibility, and to complement this Zahadat et al.(2015)believe that it is also management's responsibility to set correct policy frameworks for the BYOD .They further argue that an employee who participates in BYOD has a responsibility to ensure the security of the device they carry.

The objective of this paper is to investigate the individual traits of banking employees that will contribute to the BYOD information security culture (BYOD IS). The realisation that BYOD IS is now more than just a policy or technical issue but rather an issue that is an integral part of the overall IS strategy for the organisation motivated the theme for this paper. The individual traits associated with BYOD IS were identified through a literature review. These traits were then tested making use of a survey conducted in the banking sector in Zimbabwe. The paper further discusses the traditional IS responsibility of the information technology (IT) department and the new responsibilities that BYOD introduces to the IT department and employee as well as management. The paper recommends from that the regulatory authorities come closer to the IS policy frameworks in banks since BYOD is now beyond the banks' network perimeters. An overview of the research methodology followed in this paper will also be discussed. The paper concludes by providing an overview of the individual traits of banking employees that will contribute to the BYOD IS and discusses further research efforts to be conducted to build a case around a proposed model to improve information security culture for the BYOD unintended administrator. This positions the individual traits as fundamental components of BYOD IS culture to be discussed in detail in further research publications.

BYOD information security in the banking sector

IS is a specialized area within banking organisations and is the responsibility of the IT department (Ullman, 2011). Depending on the size of the banking organisation, some organisations will have a Chief Security Officer (CSO) who reports to the Chief Information Officer (CIO), while others have IS managers who report within the IT structures of the organisation. The IT information security officers are responsible for all IS management for the organisation. According to More et al. (2016), CSOs are responsible for both the physical and logical security of the organisation's information assets. The physical security tasks that these IT security experts perform are confined to the technical means of ensuring IS within the organisation. De state that the physical IS that the IT department can offer is limited to endpoint security, which is security of the perimeter devices in the banking network. The logical security tasks of the IT department include the formulation and enforcement of the IS policy. The responsibility also includes ensuring employee awareness and training around the organisational standards on IS.BYOD is expanding the endpoint barrier that IT security is responsible for in the banking network. Previously, the IT department had full administrative powers to monitor and control the activities on the organisational network. Different banks have different bespoke policy frameworks that satisfy their endpoint security requirements and ordinarily this is the responsibility of the organisations IT management. In Zimbabwean banks, traditional network security standards are applied variedly and audited by the organizations' internal and external auditors as per the framework created by each individual organisation. The Reserve Bank of Zimbabwe(RBZ) carries some routine audits on banks but it does not necessarily prescribe which particular framework each bank should use as it is determined by costs involved as well as the size of the organisation(Rbz, 2004).

Gundu and Flowerday (2013) recommend that there is need for organisations to cultivate positive employee security behaviour so as to mitigate the security exposures that companies face when they rely on firewalls and antiviruses which only solve part of the security problems. Employees' personal devices can now access organisational data outside the endpoint network perimeter and the employee has total control of the devices. This breaks the endpoint security barrier onto which the IT positioned the banking network. Considering that various banks are at different maturity levels in terms of their investments in IS, it is common place that the banks are impacted by BYOD with different severities(Ginovsky, 2012). It is noted from the study carried out for this paper that banks use their discretion to the satisfaction of the RBZ to implement IS policies. This paper, however, also notes that the banking industry is falling behind the BYOD IS implementation and as such there is need for a more holistic approach to catchup with the security implications which come with it.

To mitigate these security concerns, BYOD IS in banks is an area that has received a lot of attention from technology innovators who provide technology based solutions (Babatunde, Selamat, & Salman, 2014).However, little attention is paid to employees who use the devices in the BYOD phenomenon, leaving organisations exposed to risks such as device theft and data loss and even ignorance on the part of the employee regarding the importance of observing IS. Kaseya (2012)cautions that mobile devices have found their way into the banking network through the BYOD trend creating an IS crisis within the banking system. From the literature study it was identified that there is a need for employees to be involved in implementing an information security culture to support BYOD. AlHogail and Al Hogail (2015) believe that employees form a human firewall which can be used to improve IS on BYOD. In BYOD, employees are full administrators of their devices just like the IT department in the organisational network. Several propositions on models were put forward by various scholars to qualify the importance of IS in organisations.

All the models cited from the literature show the importance of an organisational culture in building IS. Chia, Maynard, and Ruighaver(2002) studied the impact of organisational culture on information security culture and proposed a model based on eight dimensions which are organisation wide, while Schlienger and Teufel(2003) analysed the security culture of organisations with a view to create and maintain an IS culture based on organisational management components. Koh, Ruighaver, Maynard, and Ahmad (2005) analysed how security governance of an organisation influences IS and formulated a model, whereas Zakaria (2004) collected data on IS research for organisations but did not specifically focus on employee traits. Alfawaz classified and organised subjects involved on information security practices but did not go to the level of employee individual traits, whilst Van Niekerk and Von Solms, (2010) believed that information security culture can be fostered into organisations through learning. It is interesting to note that the models did not specifically examine individual characteristics of the employees as contributory aspects to building an information security culture.

In this paper, bank employees are described as ‘unintended administrators’ as a result of the unintended administrative rights they have through their personal devices that contain the clients’ private information. Bank employees are now empowered to work from anywhere to allow for longer flexible hours, but this also means that banks are vulnerable to security breaches when devices are lost or data loss if they connect their mobile devices to insecure public network access points.

According to Lee, Lee, andKim(2016), IS has become a central aspect of business management such that organizations are have resorted to intensifying their information security levels. They also pointed out that government regulations are increasingly mandating organisations to observe information security as a result of the high costs of information security failures which will result in information security stress in organisations. In Zimbabwe, banks are supervised by the RBZ which falls under the Ministry of Finance. All banks are mandated to observe all policies and regulations promulgated by the RBZ to whom it is delegated by the Ministry of Finance through the Banking Act(RBZ, 2011). Garba, Armarego, and Murray (2015) stress that IS in an organisation is a complex system consisting of technical systems as well as policies and other human aspects supporting the whole process. They urged organisations to have written policies on BYOD IS as a first step in addressing the IS gap. In agreement with this perspective, Arregui, Maynard, and Ahmad (2016) point out that there is scanty research done on how policies can address the information security risks and challenges that are posed by BYOD phenomenon. They identified thirteen use cases and risks that should be addressed in order to mitigate BYOD IS risk. Noteworthy in their finding is user behaviour which constituted eight of the use cases, confirming how important the user is in formulating BYOD IS (Arregui et al., 2016).

Leavitt (2011) believes that organisations, including banks, are always playing catchup on mobile device security. In order to leverage on BYOD trends, these organizations need to revisit their strategies regarding IS. A recent survey by the Industrial Development Corporation showed that the majority of banks in both developed and developing countries are placing themselves at risk when it comes to BYOD strategies (Lund & Silva, 2015). In Zimbabwe, where the survey was conducted, the Access to Information and Protection of Privacy Act 9 Chapter 10:247 (AIPPA) makes provision for data protection by public bodies including financial organisations, such as commercial banks(DLA PIPER, 2016). The Zimbabwe Banking Amendment Act of 2015 which is the latest regulatory framework on banks is silent regarding BYOD IS which is indicative of the fact that there is a gap on the national legal framework. Whilst in Zimbabwe there are no reported cases of data breach recorded to date, this lack of information could point to a problem within the maturity levels of monitoring these breaches in the country. In South Africa, Zurich Insurance Company South Africa Ltd was fined for losing an unencrypted back-up tape during a routine transfer to a data storage center (Condon, 2015). A survey conducted by Ruvalcaba and Langin (2014)pointed out that more than two thirds of financial institutions worldwide have not optimized or deployed enterprise wide models regarding BYOD. According to a report by PWC (2015), the advent of BYOD demands that banks invest in new skills and in revamping their policies as well as customer data protection controls to manage the risks of exposures and reputational damage. Oyelakin and Olanrewaju(2016)suggest that there is a need for organisations to have a strategy that ensures the security of their information assets contained in these devices around the BYOD phenomenon. This corresponds with the recommendations from the King III report on organisational governance which mandated the responsibility of IT management to the board of directors for the organisation (King, 2009).

Banking is driven on trust where customers entrust the bank with their funds as well as other confidential details (Abend et al., 2008). IS in the banking sector is a closely guarded component as it poses a serious reputational as well as operational risk if not properly observed. Central banks are responsible for enforcing and regulating the information in banks. Downer and Bhattacharya (2016) also believe that BYOD information security is an area that has not received as much attention as compared to other IT security threats. In view of the comments above, it can be deduced that organisations that do not invest in IS for BYOD could be operating in breach of IS exposures associated with the BYOD phenomenon.

BYOD information security culture

Proponents of organisational culture positioned information security culture as a subculture of organisational culture (Lim, Chang, Maynard, & Ahmad, 2009).Da Veiga and Martins (2014)believe that "an information security culture concerns the manner in which employees perceive and interact (behave) with the controls that are implemented to protect information" (p.50). Lundy and Cowling (1996) view organisational culture as the way things are done in any particular organisation. Van Niekerk and Von Solms (2010)build on this definition when they state that information security culture is the way information security is handled in a given organisation, and The that information security culture develops as a result of employees' IS behaviour. According to Schlienger and Teufel(2003), there are three layers of information security culture which encompass all socio-cultural measures that support technical security measures so that IS becomes a natural aspect in the daily activities of every employee. Figure 1 illustrates these layers.

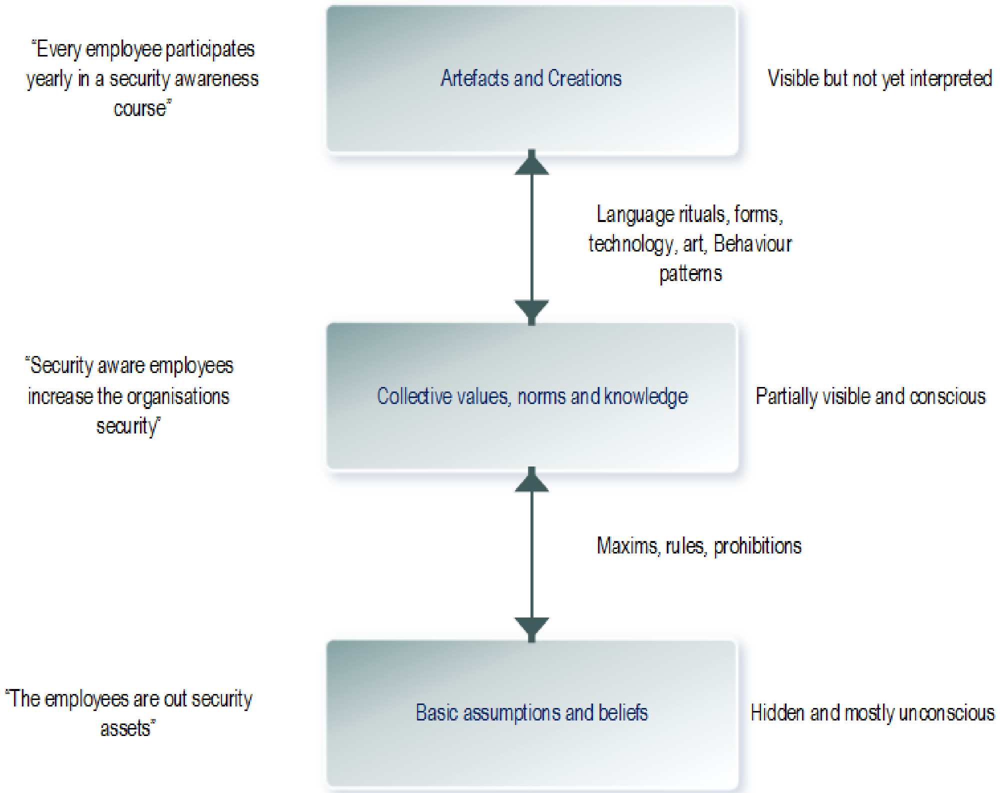

"Every employee participates yearly in a security awareness course"
Artefacts and Creations
Visible but not yet interpreted
Language rituals, forms, technology, art, Behaviour patterns
"Security aware employees increase the organisations security"
Collective values, norms and knowledge
Partially visible and conscious
Maxims, rules, prohibitions
"The employees are out security assets"
Basic assumptions and beliefs
Hidden and mostly unconscious

Figure 1:The three layers of information security culture (Schlienger& Teufel, 2003)

From this view by Schlienger and Teufel (2003), it can be deduced that the employee plays a key role in the information security culture. Da Veiga and Eloff (2010)add that the interaction between IS components like employee behavioural intentions influence the resultant information security culture in an organisation in the following three ways:

i. First by influencing the IS behaviour;
ii. Cultivating information security culture; and
iii. The creation of an information security culture.

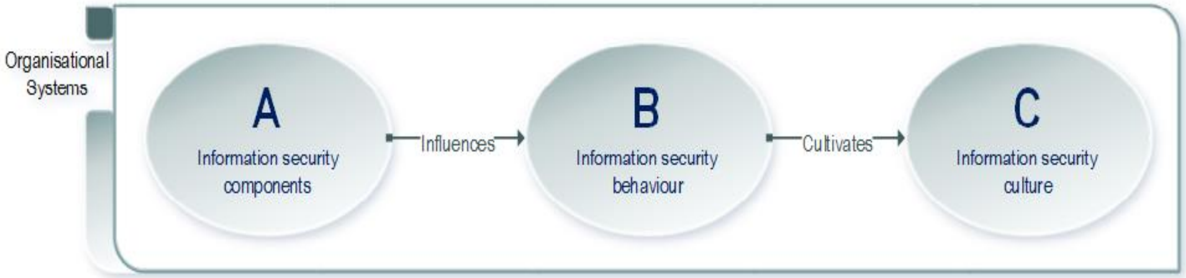

Organisational Systems
A
Information security components
Influences
B
Information security behaviour
Cultivates
C
Information security culture

Figure 2: Influencing information security behaviour and cultivating information security culture (Da Veiga & Eloff, 2010)

Figure 2 shows that information security components influences information security behaviour which in turn cultivates the information security culture. Positioning this study from the perspective of Da Veiga and Eloff (2010), it can be inferred that information security components are made up of individual components. Information security behaviour is a human component made up of information security components which will be discussed in the next section.

Information security culture individual traits

The views on information security culture from Schlienger and Teufel (2003) as well as Da Veiga and Eloff (2010) both place emphasis on the contribution by the employee in developing an information security culture. Considering that BYOD is driven by employees, it can be concluded that the solution to the security challenges that BYOD pose should also rest with the employees. However, the fact that management input on information security plays a pivotal role cannot be dismissed. From the literature on organisational culture it was learnt that employees in an organisation fit into the organisational framework (Samuel, 2015). Three major individual traits of attitude, knowledge and habit were identified to be key in building a BYOD information security culture (BYOD IS).The next section discusses these individual traits in detail. Three propositions are formulated resulting from inductive reasoning guided by findings reported in IS literature. The empirical analysis enabled the evaluation of these propositions through a case study of a commercial bank in Zimbabwe. The findings of these evaluations are discussed in the methodology section which follows.

The knowledge trait

Allam, Flowerday, and Flowerday (2014) define knowledge as what people know. In this context, knowledge can be defined as what employees know about BYOD IS, specifically about BYOD hardware, the software used to manage and drive the devices, the data contained in these devices, the policies and procedure required to optimally operate the BYOD devices, as well as the people who operate these devices. This knowledge is in essence the operational knowledge of the technical devices under use and how it fits in within the organisations IS policy framework. Operational knowledge of the devices ensures secure usage of the device; for instance, employees will need operation knowledge to understand the risks of downloading software that can be malicious to their operations (Twinomurinzi & Mawela, 2014). In a bank, Mphahlele(2016) points out that operational knowledge of the organisational policy framework is central in implementing BYOD IS.

Banking organisations recruit and appoint employees based on some inherent knowledge they possess to hold certain job profiles. Ahmed, Ragsdell, and Olphert (2011) argue that knowledge underpins the success of knowledge management initiatives within an organisation and has been recognised as a vital activity for organisational transformation and success in implementing new solutions and standards within the business. BYOD IS requires employees to be knowledgeable about the devices that they operate. In order for BYOD IS to be implemented, there is a need for the organisations (banks in this context) to invest in employee training and awareness about the consequences of not properly managing IS on their devices. D'Arcy (2011) argues that organisations require technology savvy, knowledgeable employees who can operate the new technologies, which points to the requirement of technical knowledge. The attitudes of the employees who are knowledgeable on the consequences of not observing an information security culture and those that are not knowledgeable are different. It is noteworthy that an investment in the knowledge and awareness on BYOD IS will encourage the right attitude and behaviour from employees towards IS from the attainment of technical and operational knowledge.

Safa and Von Solms (2016)state that knowledge plays an important role in the domain of information security due to its positive effect in fostering employees' IS awareness. Knowledge of the IS risks makes it easy for banking organisations to implement attendant IS policies and encourage the sharing of best practices. Van Niekerk and Von Solms (2010) argue that lack of IS knowledge on the part of the employees is detrimental to the organisation, and as such organisations have to invest in employee IS knowledge. Based on these literature review findings, the proposition on knowledge as an individual traits influencing the improvement of an IS culture for the BYOD phenomenon were formulated and then tested.

Proposition P1*: Employee operational and technical knowledge about IS is positively associated with the building of an information security culture in the BYOD phenomenon.*

The attitude trait

According to Allam et al. (2014), attitude is what people think. In this paper, attitude is what employees think about BYOD IS which includes the technology they use, the organisational policy framework they follow and how they follow it. Attitude determines the employee information security culture as it influences the level at which they observe the policy frameworks and rules surrounding its implementation (Van Niekerk& Von Solms, 2010). According to Lennon (2012), attitude can either be positive or negative. In this paper we examine the development of a positive attitude towards BYOD IS for the banks in Zimbabwe. The theory of planed behaviour (TPB) claims that the intended behaviour influences the attitude towards that behaviour. If applied to this paper it points to the fact that the attitude that the employees have towards BYOD IS and the organisational policies determines how IS can be improved in banks (Ajzen, 1991).

Regarding attitude, Da Veiga and Martins(2014) maintain that an IS culture consists of employees' attitude and beliefs with respect to IS. Furthermore, IS culture consists of knowledge of the organisation's IS policy as well as a compliancy requirement. In agreement with this perspective, Alfawazand and Nelson (2010)propose IS behaviour modes that organisations must observe in building an information security culture. Chen, Ramamurthy, and Wen (2015) believe that IS culture is an assemblage of shared security values, beliefs and assumptions in IS in the organisation and can lead to unconscious, continuous and habits that formulate the behavioural intention toward information security culture. Lee et al.(2016) state that employee attitude to compliance with the information security policies and standards within the organisation mitigates work overload and invasion of privacy, which they formulated into a model for formulating an information security stress management model. Based on these viewpoints the proposition below was tested.

Proposition P2: *The employee attitude towards BYOD IS, technology, policies and procedures is positively associated with the building of an information security culture in the BYOD phenomenon.*

The habit trait

Social theorists from Weber to Bourdieu have agreed that most of the time people in the world act habitually, not reflectively (Hopf, 2010). Vance, Siponen, and Pahnila, (2012)define habit as a routinized form of past behaviour, while Pahnila, Siponen, and Mahmood(2007) view habit as unconscious or automaticbehaviour. The habits that employees develop in using their BYOD are part of the three individual traits identified in the literature. Chen, Li, Hoang, and Lou (2013) argue that banking organisations should consider employees' habits when dealing with BYOD IS. Employees develop certain routines in dealing with information assets that collectively have an influence on habitual perceptions which inform how the information security cultures for an organisation can be improved. With BYOD this is even more important as employees will also develop habits or routines on their private devices at home which will translate into workplace practice. How the employee secures their private phone in regards to physical access or authorization to access the phone at home is unlikely to change when they enter the workplace. Following this lead, we suggest that habitual behaviour explains information security culture for individuals in any banking organisation.

Proposition P3*: The habits that employees practice towards IS are positively associated with the building of an information security culture in the BYOD phenomenon.*

These three traits of knowledge, attitude and habit will collectively constitute the individual traits of the IS culture for the BYOD unintended administrator in this paper. From the viewpoints given by the scholars above, it can be proposed that for an organisation to improve IS culture for the BYOD unintended administrator, the employee attitude, knowledge and habit towards security are indeed key individual traits. These propositions will be subjected to statistical tests. Whilst the focus of this paper is on individual traits, the next section gives a high-level discussion on the organisational traits as they also contribute towards improving BYOD IS. Details of the organisational traits will be discussed in future research work.

Organisational IS culture traits

IS culture also includes organisational traits which must be considered in the context of BYOD. While these organisational traits are not the focus of this paper, they will be briefly discussed in this section. Organisational traits include the micro environment which was identified to be one of the key role players in the formulation of employee behavioural intention (Gordon, 1991). Vignesh and Asha (2015) point out that the massive penetration of mobile devices like smartphones, tablets and phablets have changed the business environment. The highly dynamic banking environment is characterised by complex competitive practices where an employee finds derivative values that correspond to institutionalising the means by which the organisations conduct their business. BYOD is one such derivative value which is giving employees the latitude to work flexibly(Köffer & Fielt, 2015).

Organisational governance is another key component identified to have an impact on IS culture.IS management theorists assert that employee behaviour needs to be directed and censored to ensure amenability to organisational IS standards(Vroom & Von Solms, 2004;Dhillon, Tejay, Hong, & Vegas, 2007; Rastogi & VonSolms, 2012). The research findings by Da Veiga and Martins(2014) identified that IS culture in the banking sector is a prerequisite for good governance and the application of an effective regulatory framework. Vignesh and Asha (2015) further caution that there is an urgent need for organisations, including banks, to modify their IS governance policies so as to fit in with the challenges that come with BYOD. A study by Kufandirimbwa, Zanamwe, Hapanyengwi, and Kabanda(2013) on the IS of the banking sector in Zimbabwe considered governance to be a key organisational function that needed to be reinforced so as to ensure the functional Intergration of the of systems and structures. In the context of BYOD for banks, a good governance system will improve IS, thereby forming an IS culture for the BYOD unintended administrator.

Awareness training of the IS plan for the organisation is another key component which came up from the literature study as a pillar in building an IS culture. Al-shehri (2012)states that employees come from different backgrounds and that most of lack awareness towards the consequences of breaching IS guidelines. Lim, Ahmad, Chang, and Maynard (2010) warn that IS awareness is different from training in that training is more formal and confined to classrooms whereas awareness is more relaxed and very informational. Awareness teaches employees to be conscious about the IS culture in an organisation. Further, organisations may not achieve high levels of IS culture if awareness is low among employees (Lim et al., 2010).

The next section will address the design of the research instrument with special attention on the traits identified from the literature review. From the literature, BYOD IS for the unintended administrator can be defined as the way BYOD IS is managed in a bank with a special focus on individual traits of knowledge, attitudes and habits. These factors are the building blocks for a model to improve the IS culture for the BYOD unintended administrator in the banking sector. The next section will address the research methodology followed for this study.

Research methodology

Research is guided by the philosophical paradigm which outlines the philosophical underpinnings and the intellectual structure as well as the underlying assumptions which form the baseline for the research (Göktürk, 2005). The methodology followed in this research is in the form of a case study. Yin (2004) maintains that in order to investigate important topics that cannot be easily covered by other methods, it is important to carry out case study research, and doing case study research will not be different from using other research methods. The only difference between case study research and other methods is that when doing case studies there is need to do data collection and data analysis together. All methods require reviewing the literature, defining research questions and analytic strategies, using formal data collection protocols or instruments, and writing good research reports. The main data collection method used in this study is the questionnaire which was derived from the literature review.

The paper provides a review of the literature published on information security culture in BYOD as well as results from a survey conducted for a commercial bank in Zimbabwe. The identification of the three individual constructs of attitude, knowledge and habit was made through the literature survey and this guided the formulation of the research instrument which was used for the online survey. Following recommendations from Yin (2004), the case was defined as identifying traits for improving BYOD IS. A single case study was decided for a commercial bank in Zimbabwe. The findings from the case study culminated in the selected traits which were then tested using statistical techniques reported in the methodology section. Teddlie and Yu (2007)state that the case study method is best applied when researching and aims to produce a first-hand understanding of people and events. This research seeks to understand means by which banks in Zimbabwe can improve their BYOD IS, hence it was deemed relevant.

Research instrument

Data was collected using a research instrument that contained three sections. A pilot survey was conducted on 30 participants to test the clarity and user friendliness of the questions. Feedback from the pilot study was used to improve the layout and questions. After the changes, the main research instrument was developed with section 1 (6 questions) which solicited for information on the employees' demographics. Section 2 (21 questions) solicited for responses on the 3 identified traits. Finally, section 3 contained one open-ended question to capture any outstanding additional information around the BYOD phenomenon. The questions in section 2 were derived from the literature review addressing the three traits of attitude (9 questions), knowledge (7 questions), and habit (5questions). A five-point Likert-scale was used for all items, with a range from one (1=strongly disagree) to five (5=strongly agree).

The questionnaire was uploaded on an online survey developed using Survey Monkey and emailed to 270 employees of the bank. A total of 205 employees participated in the survey which was a response rate of 87%. After data cleaning it was found that 13% of the questionnaires were not completed and could not be used in the study, therefore only 179 responses were included in the final data analysis. Individual traits contributing towards the improvement of IS culture in BYOD for the unintended administrator in the bank were identified and tested in SPSSv23.Statistical analysis was conducted to refine the factors picked from the literature review. The next section will discuss the reliability and validity of the identified traits.

The data collection survey

The questionnaire was administered to bank employees for a commercial bank in Zimbabwe. Subjects were asked to indicate their agreement levels to the questionnaire formulated based on the seven traits. All the variables data collected were first coded and purified to simplify the factor structure following the suggestion by Churchill (1979).

From the survey results, about 60% respondents were males and 40% were females. The largest number of participants was between 30 and 40 years of age (55%), followed by the 41 to 50 age group (21%). Most of the employees owned mobile devices constituting 89% of all the employees. Almost all the employees (92%) confirmed that they understand the distinction between personal and organisational data and were able to keep them wholly separate while using a personal device for work. Table 1 shows the summary of the respondents' demographics.

Table 1: The demographic profile of respondents

Item	Category	Frequency	Percentage (%)
Gender			
	Male	*106*	*59.2*
	Female	*72*	*40.4*
	*Did not Indicate**	*1*	*0.6*
	Total	*179*	*100*
Age			
	<30	*29*	*16.2*
	30-40	*99*	*55.3*
	41-50	*37*	*20.7*
	>51	*14*	*7.8*
	Total	*179*	*100*
Employees who own a mobile device			
	Yes	*159*	*88.8*
	No	*18*	*10.1*
	*Did not Answer**	*2*	*1.1*
	Total	*179*	*100*

I understand the distinction between personal and organisational data and am able to keep them wholly separate while using a personal device for work			
	Yes	*165*	*92.2*
	No	*11*	*6.1*
	*Did not answer**	*3*	*1.7*
	Total	*179*	*100*

**Respondents did not specify*

The Bartlett's test of Sphericity relates to the significance of the study and thereby shows the validity and suitability of the responses collected to the problem being addressed through the study. For factor analysis to be recommended suitable, the Bartlett's test of Sphericity must be less than 0.05. The obtained result of 0.00 shows that the factor analysis is an acceptable form of analysis for this study. In addition, the KMO test was found to be above 0.6, which means the sample was acceptable for factor analysis.

In order to test the relationship between the variables identified in the literature review, a multivariate correlation was computed and the results are contained in Table 5. From the literature review it was concluded that there is a strong correlation between behavioural intention and the other six variables. In this paper, behavioural intention is viewed as a measure of the employees' intention to improve the IS culture for the BYOD unintended administrators.

Ensuring reliability and validity

The Cronbach's alpha test was used to test the reliability of the questionnaire. Carolina et al. (2003)recommend a reliability of 0.70 as extensive and one above 0.80 as exemplary. A high Cronbach alpha coefficient suggests that the scale used is reliable. The values of 0.70 and above represent a good level of reliability, whereas values between 0.50 and 0.69 are considered to have an acceptable level of reliability (Pallant, 2011). Therefore, the cut-off point of 0.50 was chosen as the measure of reliability in this study. Table 2 below examines the individual participation of the three individual traits for improving an information security culture.

Table 2: Reliability of the attitude scale

Total Cronbach's Alpha:0.803				
Original Values	**Renamed Values**	**Factor Loading**	**Item total Correlation**	**Cronbach's Alpha after del.**
6.Attitude	ATT1	.771	.766	.756
7.Attitude	ATT2	.759	.746	.759
1.Knowledge	ATT3	.710	.680	.763
4.Knowledge	ATT4	.684	.496	.784
1.Attitude	ATT5	.635	.653	.767
4.Attitude	ATT6	.600	.462	.788
9.Attitude	ATT7	.556	.554	.780
6.Knowledge	ATT8	.502	.425	.792
3.Knowledge	ATT10	.493	.481	.786
2.Knowledge	ATT11	.462	.326	.802
1.Habit	ATT12	-.444	-.254	.860

Of the nine variables originally intended to measure attitude from the SPSS factor analysis, twelve variables loaded. These twelve include some of the variables from knowledge and habit. Table2 illustrates twelve of the attitude variables to be measured renamed from ATT1 to ATT12.Eleven of the factors loaded well with the twelfth item showing a negative loading, suggesting that ATT12 does not have a positive association with the behavioural intent and attitude construct. From the statistics it can also be derived that attitude has a Cronbach's alpha coefficient of 0.803.Sufficient evidence of validity for this scale is provided.

Table 3: Reliability of habit as a scale

Cronbach's Alpha:0.610				
Original Values	**Renamed Values**	**Factor Loading**	**Item total Correlation**	**Cronbach's Alpha after del.**
4.Habit	HAB1	.656	.499	.487
3.Habit	HAB2	.627	.432	.525
5.Knowledge	HAB3	.610	.386	.552
5.Attitude	HAB4	.534	.216	.618
6.Habit	HAB5	.534	.355	.579
5.Habit	HAB6	.461	.245	.606

Table 3 illustrates that all six of the items (HAB1, HAB2, HAB3, HAB4, HAB5 and HAB6) intended to measure the habit construct variables loaded together with some of the knowledge and habit values loading. Habit had factor loadings between 0.461 and 0.656.Sufficient evidence of validity for this scale is provided. The Cronbach's alpha coefficient returned for this factor was 0.610, which is greater than the 0.5, the chosen cut-off point for this study, indicating that the scale measuring this factor is reliable. In this study, the habit construct measures employee habits towards the IS in BYOD. The validity for the habit construct was summarised in detail in Table 2.

Table 4: Reliability of knowledge as a scale

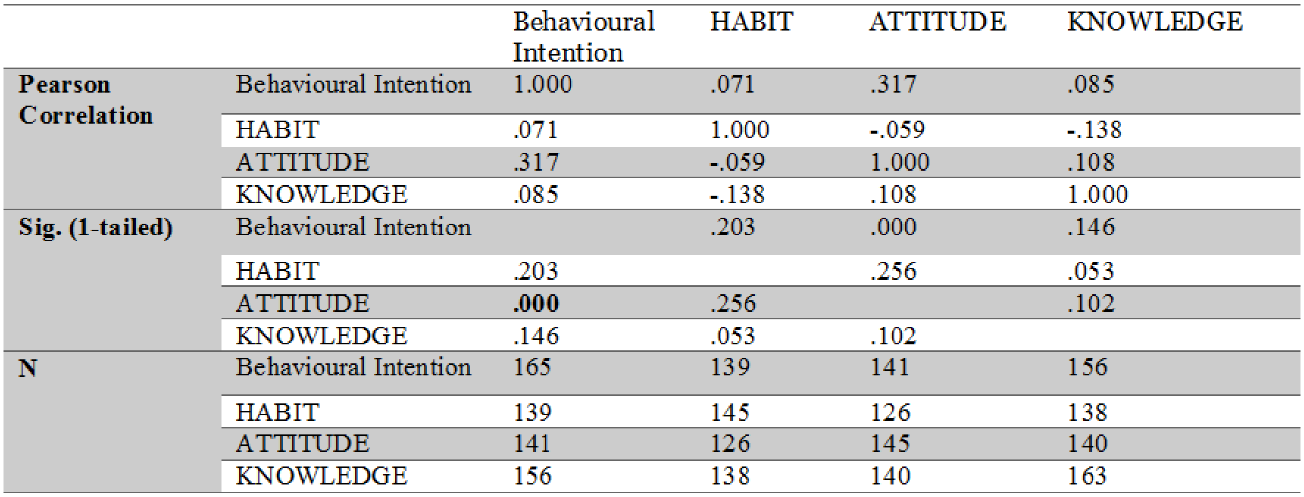
Cronbach's Alpha:-0.81				
Original Values	**Renamed Values**	**Factor Loading**	**Item total Correlation**	**Cronbach's Alpha after del.**
2.Habit	KNO1	.676	.069	-.244a
3.Attitude	KNO2	-.645	-.299	.369
2.Attitude	KNO3	.479	.101	-.323a
8.Attitude	KNO4	.407	.066	-.284a
2.Habit	KNO5	.676	.069	-.244a
8.Attitude	KNO6	.612	0.462	0.758

It can be read from Table 4 that items KNO1 to KNO6 intended to measure the employee knowledge on the IS culture aspects around BYOD. The knowledge construct did not load as expected. It has a Cronbach's alpha of -0.81, suggesting the need to recode the variable items in the opposite direction. Based on the factor loadings and the Cronbach's alpha coefficient reported, there is insufficient evidence of validity and reliability for this construct. In this study, knowledge refers to employee knowledge of IS on BYOD. This construct will, however, remain valid based on the findings from the literature study. The justification for retaining this construct will be explored in the discussion section of this paper. Additional tests were conducted on these traits so as to establish the level of participation by the three individual traits in improving an IS culture for the BYOD unintended administrator. The following section explores these additional tests.

Correlation among traits

In order to verify whether the three traits identified in the literature study could also be derived from the survey results, the Pearson product-moment correlation coefficient was carried out to measure the strength of the linear relationship between the variables. The results from R-values from the tests were computed and are displayed in Table 5. From the results, only attitude shows a significant correlation, suggesting that it is the variable which contributes more towards behavioural intention in this survey.

Table 5: Correlation among information security traits



		Behavioural Intention	HABIT	ATTITUDE	KNOWLEDGE
Pearson Correlation	Behavioural Intention	1.000	.071	.317	.085
	HABIT	.071	1.000	-.059	-.138
	ATTITUDE	.317	-.059	1.000	.108
	KNOWLEDGE	.085	-.138	.108	1.000
Sig. (1-tailed)	Behavioural Intention		.203	.000	.146
	HABIT	.203		.256	.053
	ATTITUDE	**.000**	.256		.102
	KNOWLEDGE	.146	.053	.102	
N	Behavioural Intention	165	139	141	156
	HABIT	139	145	126	138
	ATTITUDE	141	126	145	140
	KNOWLEDGE	156	138	140	163

The inferential statistics included calculating Pearson's product- moment correlations, performing both a simple and multiple regression analysis. The next section shows the product moment correlation coefficients between the variables.

Tables 6: Pearson's product moment correlation coefficients

Factor	**1= Attitude**	**2=Habit**	**3=Knowledge**
Attitude	1		
Habit	-.059	1	
Knowledge	**.108**	-.138	1

(P<0.05)

From the three individual traits, the table shows that there is a strong correlation between knowledge and attitude. Knowledge and habit show a negative correlation suggesting an inverse relationship. From Table 5 no significant correlations amongst the three traits can be identified as all the values remained significantly low. Some even show a weak negative correlation, suggesting no significant relationships between the variables. The relationships between the variables and the dependent variable of behavioural intention, however, is interesting as shown in Table 4 and examined under the discussion section of this paper.

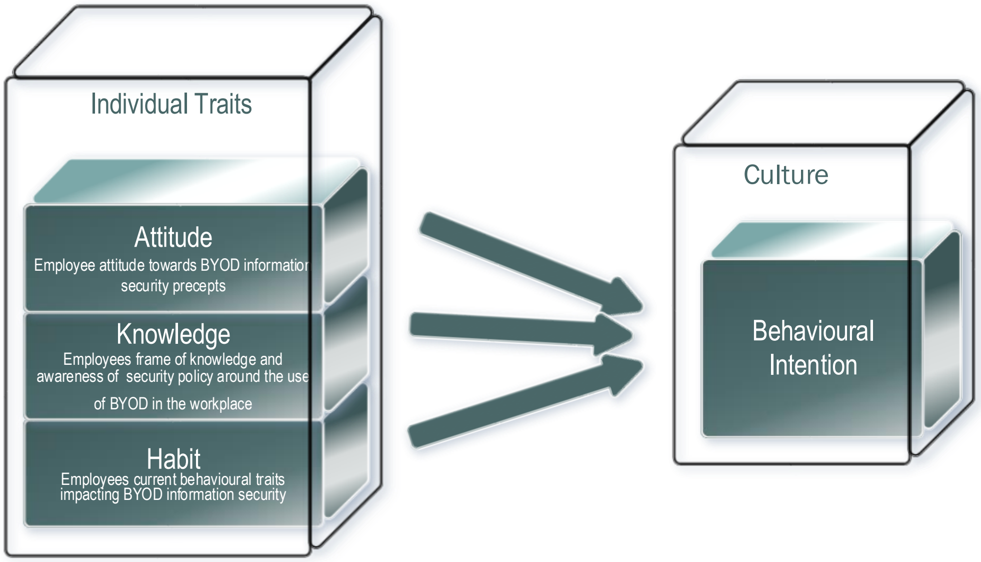

Individual Traits
Attitude
Employee attitude towards BYOD information security precepts
Knowledge
Employees frame of knowledge and awareness of security policy around the use of BYOD in the workplace
Habit
Employees current behavioural traits impacting BYOD information security
Culture
Behavioural Intention

Figure 3: The relationship between individual traits and behavioural intention (The BYOD IS model on individual traits)

Figure 3 shows the relationship between the individual traits and the behavioural intention towards IS culture. It can be seen from the figure that the three individual traits all contribute the IS culture formulation. The P-values showing this relationship are contained in Table 6. It can be inferred from the literature that the three traits of knowledge, attitude and habit have a significant bearing in the improvement of BYOD IS in banks. Figure 3 shows that the behavioural intention of employees to improve BYOD IS rests in their attitude towards the devices and polices, their knowledge of the security and repercussions of not observing it as well as their habits will collectively influence the culture The next sections contains the discussion and conclusion of the paper based on the analysis above.

Discussion: Individual traits contribution to BYOD IS

From the literature study it was inferred that for organisations to improve their BYOD IS, there is a strong participation by the individuals that make up these organisations who are referred to as unintended administrators in this discussion. The organisational environment governance also plays a central role in BYOD IS. In this paper, focus was on the three traits of attitude, habit and knowledge as identified in the literature. Each of these factors will be discussed per paragraph so as to explain their contribution.

- **Knowledge:** Based on the literature study, knowledge was identified as a key component as it explains what employees know about BYOD IS operationally and technically. In improving BYOD IS, it is noteworthy that the knowledge that employees have will play a significant role. With the confirmation by Ahmed et al. (2011) that knowledge underpins the projection of the organisation's success in implementing its policies, a high level of confidence can be achieved in confirming that knowledge is a key individual trait for improving BYOD IS. Whilst overwhelming evidence exists as proof on the importance of knowledge in improving BYOD IS, other statistical analysis measurements did not confirm this trait as a valid one. The correlation coefficient between knowledge and attitude, however, was significant. This statistic on correlation confirms the findings from the literature survey by D'Arcy (2011) as well as by Boshoff, Elizabeth, Africa, and Niekerk (2011) that knowledge is what determines employees' level of awareness of the new policies. Therefore, proposition P1: *Employee operational and technical knowledge about IS is positively associated with the building of an information security culture in the BYOD phenomenon* is accepted. It is also important to note that this proposition positively associated with the attitude of the employee when building an IS culture in the BYOD phenomenon as shown in Table 6.

- **Attitude:** Based on the comparison between the literature findings and the statistical analysis, the construct of attitude was deemed to be a key aspect in improving BYOD IS. The proposition on attitude seeks to establish how the employee attitude towards IS impacts BYOD IS. Several authors agree that the employees' attitude explains how they think towards IS policies(Flowerday& Tuyikeze, 2016;Woretaw & Lessa, 2012;Andress, Leary, Andress, & Leary, 2017). In order to improve the IS culture for the BYOD, banks need to explore this trait in employees. From the literature review it was also noted that employee attitude also influences employee beliefs. In turn, beliefs determine the rate at which the employees can adopt and implement IS conscious behaviour. Statistical analysis of the survey data confirms that attitude is a key component for BYOD IS. Attitude gave the highest reliability from the Cronbach's alpha tests with a value of 0.803 which confirms that attitude is a reliable trait in improving BYOD IS for the bank where the study was conducted. The correlation between attitude and behavioural intention gives a positive relationship with an R-value of 0.317, confirming the findings from the literature study. Figure 1 shows the relationship that culminates from the literature studies which were there confirmed statistically. The second proposition, P2: *The employee attitude towards BYOD IS, technology, policies and procedures is positively associated with the building of an information security culture in the BYOD phenomenon,* is accepted.

- **Habit:** Employee habit was identified as one of the key traits and the literature survey and statistical analysis of the survey results confirmed the findings. From the literature studies, it was noted that employee habit is unconscious and often automatic, which suggests that it is an inside component of the employees' day- to- day operations. BYOD IS will require an examination of the bank employee's day- to- day habits in order to be improved. Chen et al.(2013)state that employee routines emanate from their habits. From the statistical analysis, the habit trait accounted for a reliability of 0.610. The statistical analysis of the survey results showed the scale was reliable but not significant, therefore it should still be considered as significant in the improvement of the employees' BYOD IS. It can thus be concluded that for banks to improve their BYOD IS the employee habit trait should be considered closely as it plays a key role. The third proposition, P3: *The habits of the employee towards IS*, is positively associated with the building of an IS culture in the BYOD phenomenon as reliable in the context of BYOD, but not significant to build an IS culture within the bank for the BYOD phenomenon.

The implication here could be that for IS in the BYOD to be improved, there is need for an IS culture .As a result, it can be assumed based on the findings of this work that BYOD IS serves as a useful conceptual tool for improving IS culture on BYOD. The findings of this research can be considered useful for CISOs and boards of directors given the limited empirical evidence in the implementation of IS on the BYOD (BankingTech, 2016). In Zimbabwe where it is evident that there is no particular and specific legal frameworks addressing BYOD IS in banks, it is imperative that the RBZ pay particular attention to addressing that gap.

Limitations and future works

Future works will examine organisational traits and the impact of the improvement of BYOD IS and combine them with the individual traits discussed in this paper to create a model for building an IS culture for the BYOD unintended administrator. The survey was confined to a commercial bank in Zimbabwe which means that the different cultures that individual banks have were not examined. Whilst the bank examined is a regional bank, the study was only confined to Zimbabwe and it can be assumed that the model is only applicable to Zimbabwe. Future works will include a wide population of banks in Zimbabwe and abroad. Additional statistical tests on the model will be conducted so as to bring the empirical evidence of the model and application to the banking sector. Confirmatory tests will also be conducted to scientifically and rigorously prove the contribution from the six traits for the model. Further, future works will focus on organisational traits for building an IS culture. The organisational and individual traits will then be combined to form a model for building an IS culture for the BYOD unintended administrator.

Summary and conclusion

The papers begins by acknowledging that the modern day IS management is the sole responsibility of IT employees who require special skills to manage it with the management playing catchup in implementing the requisite policy frameworks. The fact that BYOD violates existing IS boundaries is cited as the main reason why organisations need to invest in improving their IS culture. The banking sector in Zimbabwe was used as the base on which this study was conducted. Firstly, a literature study was conducted, leading to the identification of three individual traits of attitude, knowledge and habit. Three propositions were formulated per each construct followed by a statistical analysis of the results obtained from a survey of 270 employees from a commercial bank in Zimbabwe. A brief discussion linking the literature review findings and the statistical analysis was conducted for the three traits. This culminated into the recommendation of the three traits in the improvement of BYOD IS.

This paper concludes by recommending that banks should make it the responsibility of every employee to take charge of the security of its information asserts by building an IS culture for the BYOD phenomenon. The paper also recommends that a specific legal framework be created to improve the IS culture in the BYOD phenomenon. The approach on IS by which banks tailor make their own policy frameworks is deemed a big gap as BYOD now operates at a global scale threatening the security for the whole banking industry. The comfort that the banks used to enjoy in controlling data through endpoint security has since been overtaken by the BYOD phenomenon. For banks to implement a model for improving BYOD IS they need to address the employees' individual traits, which are knowledge, attitude and habit, which will then be backed by a legal framework that support them. The success of banks improving their IS culture has been found in this research to be dependent on individual and organisational traits that influence the organisational information security culture. Employees have been identified to be key stakeholders in the improvement of IS in BYOD for banks. Based on this realization, BYOD IS provides a practical and technology independent solution to improve the IS culture for the BYOD unintended administrator.

References

Abend, V., Peretti, B., Bach, A., Barry, K., Donahue, D., Wright, K., … Axlerod, C. W. (2008). Cyber Security for the Banking and Finance Sector. … *Homeland Security*, 1–17. http://doi.org/10.1002/9780470087923.hhs460

Abramson, J. (2014). *BYOD: A Potential Cybersecurity Nightmare*.

Ahmed, G., Ragsdell, G., & Olphert, W. (2011). Knowledge Sharing and Information Security: A Paradox? *European Conference on Knowledge Management*, 1083–1091.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processess*, *50*(2), 179–211.

Al-shehri, Y. (2012). Information Security Awareness and Culture. *British Journal of Arts and Social Sciences*, *6*(1), 61–69.

Alfawaz, S., & Nelson, M. (2010). Information security culture : A Behaviour Compliance Conceptual Framework. *Proceedings of the . 8th Australasian Information Security Conference (AISC 2010)*, *105*(Aisc), 47–55.

AlHogail, A., & Al Hogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. http://doi.org/10.1016/j.chb.2015.03.054

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56–65. http://doi.org/10.1016/j.cose.2014.01.005

Andress, J., Leary, M., Andress, J., & Leary, M. (2017). Chapter 10 – Information Security Program Metrics. In *Building a Practical Information Security Program* (pp. 169–183). http://doi.org/10.1016/B978-0-12-802042-5.00011-1

Arregui, D. A., Maynard, S. B., & Ahmad, A. (2016). Mitigating BYOD Information Security Risks. *Australasian Conference on Information Systems 2016*, 1–11.

Babatunde, D. A., Selamat, M. H., & Salman, R. T. (2014). The Role of Information Security Development (ISD) in Effective Information Security Management (ISM) Implementation in the Banks: A Nigerian Case, *10*(5), 614–619.

BankingTech. (2016). BYOD – Harnessing the Opportunity Securely » Banking Technology. Retrieved July 30, 2016, from http://www.bankingtech.com/49879/byod-–-harnessing-the-opportunity-securely/

Boshoff, R., Elizabeth, P., Africa, S., & Niekerk, J. Van. (2011). Defining a " generic " end -user : An Information Security perspective.

Carolina, S., Carolina, S., Yi, M. Y., & Davis, F. D. (2003). Developing and Validating an Observational Learning Model of Computer Software Training and Skill Acquisition.

Chen, A. H., Li, J., Hoang, T., & Lou, X. (2013). Security Challenges of BYOD : a Security Education , Training and Awareness perspective, 1–8.

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. (2015). IMPACTS OF COMPREHENSIVE INFORMATION SECURITY PROGRAMS ON INFORMATION SECURITY CULTURE. *The Journal of Computer Information Systems*, *55*(3), 11.

Chia, P. a., Maynard, S. B., & Ruighaver, a. B. (2002). Understanding Organizational Security Culture. *Pacis*, 1–23. Retrieved from http://people.eng.unimelb.edu.au/seanbm/research/2003SecCultChap.pdf

Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research*, *16*(1), 64. http://doi.org/10.2307/3150876

D'Arcy, P. (2011). CIO strategies for consumerization: The future of enterprise mobile computing. *Dell CIO Insight Series*, 1–15.

Da Veiga, A., & Eloff, J. H. P. (2010a). A framework and assessment instrument for information security culture. *Computers & Security*. Elsevier. http://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Eloff, J. H. P. (2010b). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. http://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N. (2014). Information Security Culture : A Comparative Analysis of Four Assessments. *Proceedings of the 8th European Conference on IS Management and Evaluation University of Ghent, Belgium*, 49–57.

Dhillon, G., Tejay, G., Hong, W., & Vegas, L. (2007). Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations, 1–9.

DLA PIPER. (2016). Data Protection Laws of the World, (December), 509. Retrieved from https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all

Downer, K., & Bhattacharya, M. (2016). BYOD Security : A New Business Challenge. *5th International Symposium on Cloud and Service Computing (SC2 2015).* http://doi.org/10.1109/SmartCity.2015.221

Eschelbeck, G., & Schwartzberg, D. (2012). *BYOD risks and rewards:How to keep employee smartphones, laptops and tablets secure*. *Sophos Whitepaper*.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. http://doi.org/10.1016/j.cose.2016.06.002

Garba, A. B., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences*, *10*(3), 1279–1287. Retrieved from http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0215_1591.pdf

Gens, F., Levitas, D., & Sega, R. (2011). 2011 Consumerization of IT Study : Closing the " Consumerization Gap ." *Idc*, *1156*, 1–21. Retrieved from http://www.unisys.com/iview

Ginovsky, J. (2012). "BYOD" quandary- when the bring your own device trend comes to the bank,measures the sisks carefully. *ABA Banking Journal*, (Tech Topics| Office Tools).

Göktürk, E. (2005). *What is " paradigm "?* Retrieved from http://folk.uio.no/erek/essays/paradigm.pdf

Gordon, G. G. (1991). Industry Determinants of Organizational Culture. *Academy of Management Review*, *16*(2), 396–415. http://doi.org/10.5465/AMR.1991.4278959

Hopf, T. (2010). The logic of habit in International Relations. *European Journal of International Relations*, *16*(4), 539–561. http://doi.org/10.1177/1354066110363502

Kaseya. (2012). Mobile & BYOD Technology Trends in Financial Services. *Kaseya Whitepaper*.

King, M. (2009). Principles for South Africa. *Institute of Directors in South Africa*, *1*(9), 1–141.

Köffer, S., & Fielt, E. (2015). IT Consumerization and its Effects on IT Business Value , IT Capabilities , and the IT Function.

Koh, K., Ruighaver, a., Maynard, S., & Ahmad, a. (2005). Security Governance : Its Impact on Security Culture. *Proceedings of The Third Australian Information Security Management Conference*, 1–12. Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2005/aism/koh.pdf

Kufandirimbwa, O., Zanamwe, N., Hapanyengwi, G., & Kabanda, G. (2013). Mobile Money in Zimbabwe : Integrating Mobile Infrastructure and Processes to Organisation Infrastructure and Processes. *Online Journal of Social Sciences Research*, *2*(4), 92–110.

Leavitt, N. (2011). Mobile security: Finally a serious problem? *IEEE Computer Society*, *44*(6), 11–14. http://doi.org/10.1109/MC.2011.184

Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the Influence of Security, Privacy, and

Legal Concerns on Employees' Intention to Use BYOD Mobile Devices. *Amcis*, (2008), 1–8. Retrieved from http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/8/

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security*, *59*, 60–70. http://doi.org/10.1016/j.cose.2016.02.004

Lennon, R. (2012). Changing user attitudes to security in bring your own device (BYOD) & the cloud. *Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania*, 49–52. http://doi.org/10.1145/2384716.2384771

Lim, J. J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. *Pacis 2010*, 463–474. Retrieved from http://www.pacis-net.org/file/2010/S11-03.pdf%5Cnhttp://www.scopus.com/inward/record.url?eid=2-s2.0-84855993316&partnerID=40&md5=142363e45290b5e2475ef5a60ea4fbe3

Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. *7th Australian Information Security Management Conference*, (December).

Liu, C. (2014). The enemy within: the inherent security risks of temporary staff. *Computer Fraud & Security*, *2014*(5), 5–7. http://doi.org/10.1016/S1361-3723(14)70489-0

Lund, D., & Silva, J. (2015). *Financial Services Optimizing BYOD Strategies for Success*. Retrieved from http://www.business.att.com/content/whitepaper/optimizing-byod-strategies-for-success-whitepaper.pdf

Lundy, & Cowling. (1996). Strategic human resource management.

Mphahlele, P. (2016). *The impact of Bring-your-own-device on work practices in the financial sector Information*. University of Cape Town.

Musarurwa, A., & Jazri, H. (2015). A proposed framework to measure growth of Critical Information Infrastructure Protection in Africa. *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015*, 85–90. http://doi.org/10.1109/ETNCC.2015.7184813

Oyelakin, A. M., & Olanrewaju, M. J. (2016). Towards a Secure Adoption of Bring Your Own Device (BYOD) Policy in Nigerian Corporate Organisations. *Computing, Information Systems, Development Informatics & Allied Research Journal Vol. 7*, *7*(3), 1–6.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. http://doi.org/10.1109/HICSS.2007.206

Pallant, J. (2011). *For the SPSS Survival Manual website , go to www.allenandunwin.com/spss This is what readers from around the world say about the SPSS Survival Manual :*

Pwc. (2015). *Bring Your Own Device (BYOD) and customer Data Protection- Are you ready? Contracting Business*.

Rastogi and VonSolms. (2012). Information Security Service Culture – Information Security for End-users, *18*(12), 1628–1642.

Rbz. (2004). RESERVE BANK OF ZIMBABWE MINIMUM INTERNAL AUDIT STANDARDS IN BANKING INSTITUTIONS, (2).

RBZ. Zimbabwe Banking Act (2011).

Ruvalcaba, C., & Langin, C. (2009). SANS Institute InfoSec Reading Room. *System*, (1), 19.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. http://doi.org/10.1016/j.chb.2015.12.037

Samuel, O. B. (2015). The Effects of Organisational Culture and Stress on Organisational Employee Commitment. *Management*, *5*(3), 96–106. http://doi.org/10.5923/j.mm.20150503.03

Schlienger, T., & Teufel, S. (2003). Information security culture: from analysis to change. *South African Computer Journal*, *31*, 46–52.

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

Teddlie, C., & Yu, F. (2007). Mixed Methods Sampling: A Typology With Examples. *Journal of Mixed Methods Research*, *1*(1), 77–100. http://doi.org/10.1177/2345678906292430

Twinomurinzi, H., & Mawela, T. (2014). Employee perceptions of BYOD in South Africa : Employers are turning a blind eye ? *The Southern African Institute for Computer Scientist and Information*

Technologists Annual Conference 2014 Empowered by Technology, 126–131. http://doi.org/10.1145/2664591.2664607

Ullman, E. (2011). BYOD and Security. *Tech & Learning*, *31*(8), 32–34,36. Retrieved from http://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ:education&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=article&rft.jtitle=Tech+&+Learning&rft.atitle=BYOD+and+

Van Niekerk, J. F., & Von Solms, R. (2010a). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476–486. http://doi.org/10.1016/j.cose.2009.10.005

Van Niekerk, J. F., & Von Solms, R. (2010b). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. http://doi.org/10.1016/j.cose.2009.10.005

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insight from Habit and Protection Motivation Theory. *Information & Management*, *49*(49), 190–198. http://doi.org/10.1016/j.im.2012.04.002

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. In *Procedia Computer Science* (Vol. 50). http://doi.org/10.1016/j.procs.2015.04.023

Vroom, C., & Von Solms, rossouw. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198. http://doi.org/10.1016/j.cose.2004.01.012

Woretaw, A., & Lessa, L. (2012). *INFORMATION SECURITY CULTURE IN THE BANKING SECTOR IN ETHIOPIA*.

Yin, R. K. (2004). Case study methods. *Handbook of Complementary Methods in Education Research*, 111–122. http://doi.org/10.1016/0742-051X(89)90032-2

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. a. (2015). BYOD security engineering: a framework & its analysis. *Computers & Security*, *55*, 81–99. http://doi.org/10.1016/j.cose.2015.06.011

Zakaria, O. (2004). Understanding challenges of information security culture: a methodological issue. *2nd Australian Information Security Management Conference*, 83–93. Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2004/aism/InfoSec Conference Complete Proceedings.pdf#page=83