Received: 12 July 2018 | Revised: 15 December 2018 | Accepted: 18 December 2018
DOI: 10.1002/isd2.12076

RESEARCH ARTICLE

WILEY

The bring-your-own-device unintended administrator: A perspective from Zimbabwe

Alfred Musarurwa[1] | Stephen Flowerday[2] | Liezel Cilliers[1]

[1] Department of Information Systems, University of Fort Hare, East London, South Africa

[2] Department of Information Systems, Rhodes University, Grahamstown, South Africa

Correspondence
Stephen Flowerday, Department of Information Systems, Rhodes University, PO Box 94, Grahamstown, 6140, South Africa.
Email: s.flowerday@ru.ac.za

Abstract

As bring your own device (BYOD) becomes part of workplace tools for employees in Zimbabwe, the responsibility to implement information security management methods, which was traditionally confined to the information technology (IT) employees, has extended to all the employees, who now become unintended administrators because of the usage of their devices. The purpose of this paper is to show how banks can mitigate the information security risks caused by the unintended administrator using the BYOD information security behavioural (BISB) model. A literature review of the BYOD information security and organisational information security culture was conducted. A questionnaire was developed from the literature and sent to 270 bank employees in Zimbabwe. A total of 205 employees participated, and 179 completed the questionnaire. An expert review consisting of chief information officers (CIOs) at banks in Zimbabwe was conducted to evaluate the proposed model. From the literature review, individual traits of attitude, knowledge, and habit, as well as organisational traits of the environment, governance, and training, were identified as key traits that constituted the constructs of the BISB model. The overall theme of this paper is that banks can mitigate the BYOD information security challenges by using of the BISB model.

KEYWORDS

bring your own device, BYOD information security behavioural model, information security culture, unintended administrator

1 | INTRODUCTION

The current disruptive trends in the form of bring your own device (BYOD) that have infiltrated the information technology (IT) landscape across all industries not only require that organisations upgrade the way they manage their information security (IS), but also demand that every organisation builds a solid and practical approach towards IS. These challenges come in the form of IS breaches, potential system intrusions, data losses, and improper exposures resulting from these disruptive tendencies (Garba, Armarego, Murray, & Kenworthy, 2015). Eschelbeck and Schwartzberg (2012) warned that BYOD in the workplace has become the rule rather than the exception, and the affected organisations will need to devise a strategy to mitigate the risks that BYOD introduces. Before the BYOD phenomenon became common in the workplace, the IT departments solely managed the devices organisations used to perform their business functions. The proliferation of BYOD in the workplace has extended the administrative control of these devices from the IT department to every employee of the organisation who owns such a mobile device that contains organisational data. In this paper, the employee who has administrative power over the mobile devise is called the "unintended administrator." The unintended administrator has the power to install, configure, and alter any setting on the mobile device he/she uses. This means that the IT personnel no longer have full control of the devices, and consequently, this poses a security risk. Chen (2014) warns that in this day of IS management, the mobile devices and the human beings operating the devices are the weakest link in IS. He further points out that organisations need to pay attention to the mobile devices that enter their networks because of the risks they pose.

This paper starts by providing an overview of how BYOD has affected the way IS is managed in organisations and indicates how the employees who own such devices have become unintended administrators in the BYOD phenomenon. The security risks that the unintended administrators introduce to the organisation because of BYOD forms the research problem that this paper attempts to address. The identification of individual and organisational traits forming the constructs for the BYOD information security behavioural (BISB) model is then discussed, which leads to the statistical survey that tested these constructs.

The next section discusses the background on the emergence of the unintended administrator in the workplace.

2 | BACKGROUND

BYOD is emerging as the new norm in modern business computing trends. All organisations that are serious about remaining relevant in the digital era are searching for BYOD security solutions (Brodin, 2016a). Digital transformation visionaries such as Wood (2004) and Morrow (2012) share the sentiment that IS in all organisations is now multidisciplinary, multidepartmental, and multiorganisational. This paper explores the multidepartmental nature of IS. Lim and Churchill (2016) further argue that the management of IS in earlier decades was strictly technical and fell under the exclusive management of an organisation's information technologists. Since 2010, a shift occurred away from specialised management of IS by IT administrators to the management of IS by employees in the various departments of the organisation (Keyes, 2013). The management of IS has always been viewed as an IT function in businesses in all industries. The issue of IS is thus central to organisations across different industries, which underscores the importance of proper management (Betz, 2016).

The banking industry views the matter of IS more seriously than most; breaches can have detrimental consequences when they occur in this industry sector. This is why Ginovsky (2012) cautions that when BYOD comes to banks, they should measure the risks carefully. Traditionally, organisations, including banks, used to provide all the devices used by employees to process organisational tasks (Singh & Phil, 2012). The devices could only connect to the organisational network, in which security standards were implemented and controlled by the IT department. The revolution in mobile device technology saw mobile devices also entering organisations. The advances in wireless network access points were one of the factors that accelerated the growth in the mobile device adoption in the workplace.

Currently, there is an information gap in the BYOD IS body of knowledge, especially for banks, in view of the confidentiality associated with the industry (Gustav & Kabanda, 2016). The dearth of this type of information is even more prevalent in developing countries where regulation is often seen to be playing catch-up with innovation. IS is such an integral component of banking that a small breach can have far-reaching consequences for the business. Although there are technical ways of securing the information on the BYOD devices, there is still a need for a solution that addresses the human aspect of IS (AlHogail & Mirza, 2015). Stewart, Chapple, and Gibson (2012) confirm “to understand and apply security governance, you must address the weakest link in your security chain – namely the people.” This paper therefore underscores the importance of security culture as the people component in mitigating the risks associated with the BYOD unintended administrator.

The next section provides an overview of the organisational information security culture (ISC).

3 | ORGANISATIONAL ISC

Mohanty (2015) suggests that organisational characteristics influence employee performance, while the overall organisational working environment influences the creation of an organisational information security culture (OISC). This paper views OISC as a subculture of the organisational culture (OC). Schein (2009, p. 17) defines OC as “a pattern of shared basic assumptions that a group learns as it solves its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new staff members as the correct way to perceive, think and feel in relation to those problems.” A practical description of culture is the way things are done in any particular organisation (Lundy & Cowling, 1996). From these two perspectives, this paper views OISC as the way an organisation manages and handles IS-related issues.

The way an organisation manages BYOD IS issues constitutes its organisational BYOD ISC. The paper views the BYOD OISC as important in order to mitigate the risks posed by the unintended administrator.

4 | THE IMPORTANCE OF THE OISC

Although there are technical solutions to the BYOD IS challenges, the OISC is viewed as the most effective way of mitigating the risks associated with the BYOD unintended administrator. There are several solutions that are vendor-specific, but not all solutions are interoperable enough to bring the confidence required to address the security issues concerned with the BYOD unintended administrator.

First, the OISC is platform-independent, which implies that if organisations have devices from different vendors, such as Android, Windows, or Apple IOS, the implementation of a BYOD OISC approach is platform-agnostic. An OISC is concerned with the individual who uses the device and not with the underlying technology of the device (Haworth, 2015).

Second, an organisation can grow its OISC, which confirms that the organisation can align the OISC with its overall OC. Culture grows and can be built through either the active or the passive participation of the organisational stakeholders, bearing in mind that the employee is the first building block of OC (Tharp, 2009).

Third, the investment in OISC can be grown and changed from one point, namely the employee. If a change in the OISC occurs, it affects all the technologies at once, unlike a change in the security standards, which occurs at a technical level when different vendors will have different updates for their technologies.

The three points above underscore the importance of an OISC. In order to clarify the way, the unintended administrator's use of BYOD will be secured through the OISC. The next section explores how the role profiles changed from the IT administrator to the administration of information by every employee in the organisation and briefly examines the IT administrator so as to provide insight into how the profile switched to the unintended administrator as a result of BYOD.

5 | THE IT ADMINISTRATOR

The IT administrator in this paper is the IS technologist who is a specialist in the IS matters of the organisation. The IT administrator is part of the IT team that manages the organisation's day-to-day IT functions as its core job function. The IT administrator defines and monitors the information policy standards for the organisation on behalf of every employee and has total control of what other employees can and cannot access in the organisation's IT network. The IT administrator engages IS vendors, where necessary, on behalf of the whole organisation. The IT administrator has a clearly defined job profile on the company's organogram and functions as the “intended administrator” of the information systems security.

6 | THE UNINTENDED ADMINISTRATOR

In this paper, any other employee who is not an IT administrator but is in charge of his/her mobile device and participates on the organisational network is referred to as the BYOD unintended administrator. The unintended administrator is not an information technologist and works in another department where his/her job profile is not information-technology-oriented. The fact that BYOD provides total administrative control of the devices used by the employees to connect to and access organisational information makes them administrators. The BYOD phenomenon is an employee-driven technological trend in which the employee chooses his/her own device (Brodin, 2016b). The organisation does not have the responsibility for or exercise control over the device, even though the information the device contains is pertinent to its operations. The fact that organisations did not plan or willingly afford employees this level of control based on their job descriptions makes the employees unintended administrators. Such unintended administrators pose serious IS challenges considering that they are not specialists in IS management. The next section explores the risks posed by the unintended administrator and forms the problem statement of this paper.

7 | THE RISKS POSED BY THE UNINTENDED ADMINISTRATOR

The advent of BYOD in the workplace has left many IS professionals concerned about the integrity of the organisational information (Cameron, 2012). The risks that the unintended administrator pose results in exposure of the organisation because the mobile devices are subjected to various vulnerabilities. Some of the vulnerabilities that the devices are subjected to are as follows:

First, the mobile device connects to several network access points, some of which may be rogue network points. This can open the organisation to potential attacks through the mobile device. Second, if the mobile device does not have strong security configurations and the device is stolen, the organisation may be exposed to attacks through the information on the device. The third risk is that employees often do not update their operating system patches, and most of them do not have antivirus software on the device (Arregui, Maynard, & Ahmad, 2016). Often, the unintended administrators have different device types, making it difficult to trace the update and to patch the operating system. Shumate and Ketel (2014) identified several other risks associated with the unintended administrator, including malware attacks and the loss of important documents that may be stored on such devices in the event that the employee leaves the organisation.

Because the challenges posed by the unintended administrator involve the employee and the organisation, the solution to these challenges concerns both the employee and the organisation. Therefore, inasmuch as technical security solutions to the BYOD exist, the most practical solution lies in the organisational needs as well its employees who use these technical solutions. The paper thus discusses the way the organisation should examine employees' individual traits as well as the organisational traits. The paper further recommends that a combination of these individual and organisational traits be used as constructs for a model for securing the unintended administrator. This helps to protect the organisations as they transition from IT administrators to unintended administrators.

8 | RESEARCH METHODOLOGY

The recommendations made in this paper are based on the literature review carried out on BYOD IS challenges as well as on a research survey at a commercial bank in Zimbabwe. Ethical approval was obtained from the bank where the survey was conducted and from the University of Fort Hare's Research Ethics Committee. From the literature survey conducted, six traits were identified that influence the behavioural intention of the unintended administrator to develop a culture of IS. The traits were classified as individual or organisational traits. Reliability tests, regression analysis, and correlation analysis tests were conducted; they are presented in Section 11 of this paper. The results from the literature review and the statistical tests conducted were used to form the basis for selecting the six traits.

A questionnaire Appendix 1 was compiled from the literature to evaluate how the identified traits influence the behavioural intention to observe an ISC with respect to the BYOD phenomenon in the banks. The questionnaire was loaded on SurveyMonkey, and a survey was conducted among 270 employees of a selected bank in Zimbabwe. Table 1 gives a summary of the profile for the respondents.

The profiles for the participants were also characterised by various departments within the bank. From a demographics perspective, the employees were within the employment age group of Zimbabwe, which is below 65 years of age. Approximately 60% of the respondents were males, and 40% were females. In this employment active cohort of respondents, about 89% owned mobile devices and 10% did not, whereas 1% did not indicate.

From the responses received, 92% understood the distinction between personal and organisational data as well as the importance to keep the data separate. Of this cohort, 6% did not understand the distinction while 2% did not indicate. A total of 205 employees participated in the study; 179 of the responses were deemed usable (that is, a response rate of 87%). The survey results were then subjected to statistical tests, such as factor analysis, regression analysis, and descriptive analysis. The results obtained were factored into the model proposed in this paper. An expert review process was conducted to evaluate the model.

The next section comprises the findings from the literature survey, which yielded the traits that formed the constructs for the model. Research propositions were formulated based on the traits.

9 | INDIVIDUAL TRAITS

There is a need for an organisation to make it every employee's responsibility to manage the organisation's IS (Bransford, 2000; Lanaj, Johnson, & Barnes, 2014; Pattinson, Butavicius, Parsons, Mccormac, & Jerram, 2015; Peslak, Ceccucci, & Sendall, 2012). Puhakainen and Siponen (2010) confirmed that the human component is integral, while Kruger and Kearney (2006) point out that IS training is also a key component. Employee insider computer crime was put forward as a component by Leclercg-Vandelannoitte (2015), and Vroom and Von Solms (2004) name IS policy

TABLE 1 Demographic profile of the respondents

Item	Category	Frequency	Percentage (%)
Gender			
	Male	106	59.2
	Female	72	40.2
	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 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

*Indicates a negative response.

obedience as a requirement for employees. All these studies aim at minimising the threat that user behaviour poses to the protection of information assets.

Employees can make a valuable contribution to developing an ISC (Schlienger & Teufel, 2003; Da Veiga & Eloff, 2010). From the literature study, three major individual traits were identified as central to determining the behavioural intention to implement a BYOD ISC. These traits are attitude, knowledge, and habit. In order to clarify why these traits are central to the individual behavioural intention, the next section analyses each trait in detail.

9.1 | Attitude

Attitude is defined as what employees think about BYOD IS, which includes the technology they use, the organisational policy framework they follow, and how they adhere to the policy. Allam, Flowerday, and Flowerday (2014) define attitude as "what people think." Attitude determines the employee ISC because it influences the level at which the employee observes the policy framework and rules surrounding its implementation (Van Niekerk & Von Solms, 2010). Attitude can also be either positive or negative (Lennon, 2012). In this paper, the development of a positive attitude towards BYOD IS for commercial banks in Zimbabwe is explored.

Da Veiga and Martins (2014) maintain that an ISC consists of employees' attitude and beliefs with respect to IS. Furthermore, the ISC depends on knowledge of the organisation's IS policy and compliance with it. In agreement with this perspective, Alfawaz, Nelson, and Mohannak (2010) put forward IS behaviour that organisations should observe in building an ISC.

Chen, Ramamurthy, and Wen (2015) believe that an ISC is an assemblage of shared security values, beliefs, and assumptions in IS in the organisation and can lead to unconscious, continuous habits that formulate the behavioural intention towards the ISC. Employee attitudes towards compliance with the IS policies and standards in an organisation mitigate work overload and invasion of privacy (Lee, Lee, & Kim, 2016); this was formulated into a model for developing an IS stress management model. Attitude is therefore identified as a key member trait in formulating a BYOD ISC. The following proposition was formulated on attitude as a trait.

> **Proposition P1:** *Employee attitudes towards IS is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

9.2 | Knowledge

Knowledge plays an important role in the domain of IS because of its positive effect in fostering employees' IS training (Safa et al., 2015). Separate research studies define knowledge as what people know (Kruger & Kearney, 2006; Safa, Solms, & Furnell, 2016). In this context, knowledge can be defined as what employees know about BYOD IS in a bank, as well as what the employees know about BYOD hardware, the software used to manage the devices, the data contained in these devices, and the policies and procedures required to optimally operate the devices. This knowledge is the operational knowledge. Operational knowledge of the devices ensures secure use of the device; for instance, employees will need operational knowledge to understand the risks of downloading software that can be malicious (Twinomurinzi & Mawela, 2014). In a bank, operational knowledge of the organisational policy framework is central to implementing BYOD IS (Mphahlele, 2016).

Banking organisations recruit and appoint employees based on some inherent knowledge they possess to hold certain job profiles. Knowledge underpins the success of knowledge management initiatives in an organisation and has been recognised as a vital activity for organisational transformation and success in implementing new solutions and standards in the business (Ahmed, Ragsdell, & Olphert, 2014).

BYOD IS requires employees to be knowledgeable about the devices they operate. In order for BYOD IS to be implemented, the organisations (banks in this context) need 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 employees who can operate the new technologies, which points to the requirement of technical knowledge. The attitude of the employees who are knowledgeable about the consequences of not observing an ISC and those who are not knowledgeable may differ. Notably, an investment in knowledge of and training in BYOD IS will encourage the right attitude and behaviour in employees towards IS because of their attainment of technical and operational knowledge.

Knowledge of IS risks makes it easy for banking organisations to implement attendant IS policies and encourage the sharing of best practices. Employees' lack of IS knowledge is detrimental to the organisation, and such organisations ought to invest in employee knowledge (Van Niekerk & Von Solms, 2010). On the basis of these literature review findings, the following proposition was formulated on knowledge as an individual trait.

> **Proposition P2:** *Employee knowledge is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

9.3 | Habit

Social theorists agree that, most of the time, people act habitually, not reflectively (Hopf, 2010). Vance, Siponen, and Pahnila (2012) define habit as a routinised form of past behaviour, while Pahnila, Siponen, and Mahmood (2007) view habit as unconscious or automatic behaviour. The habits that the employees develop in using their BYOD are part of the three individual traits identified in the literature. Frauenstein and Flowerday (2016) advocate that employees should process information systematically rather than heuristically, which is often based on habit. Banks should consider employees' habits when dealing with BYOD IS (Chen, Li, Hoang, & Lou, 2013). Employees develop certain routines in dealing with information assets that collectively have an effect on habitual perceptions, which inform the way an organisation's ISC can be improved. This is even more important with BYOD as employees will develop habits on their private devices at home that will extend to the workplace. How employees secure their private device with regard to physical access or authorisation to access is unlikely to change when they enter the workplace. Following this lead, this paper suggests that habitual behaviour explains the ISC for individuals in any banking organisation. The following research proposition was formulated.

Proposition P3: *The employee's habits towards IS is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

10 | ORGANISATIONAL TRAITS

Two contrasting perspectives exist for organisations to implement BYOD security (Leclercg-Vandelannoitte, 2015). The first perspective is that organisations build IT systems that users either want to use or not, while the second perspective maintains that users introduce IT systems that organisations either want to incorporate or not. This paper focuses on the employee as an unintended administrator, which is in line with the second perspective. The organisational traits identified cushion the resultant organisational traits that influence how the employee can use BYOD securely.

The literature review, which explores IS in BYOD, indicates that the management approach to BYOD IS and the environment combined with the training and awareness given to the employees affect the behavioural intention to implement IS. This informs the three organisational traits of environment, governance and training. The combination of these traits culminates in the organisational behavioural intention to implement security, which in this context is viewed as an ISC.

10.1 | Environment

While the right environment is associated with a better ISC, the massive penetration of mobile devices, such as smartphones, tablets, and phablets, has changed the business environment (Farooq & Amin, 2017; Vignesh & Asha, 2015). 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 that gives employees the latitude to work flexibly (Köffer Fielt, & Niehaves, 2015).

The environment determines the level of sophistication as well the rate at which the BYOD security is propagated (Farooq & Amin, 2017). The absence of a uniform approach to adopting BYOD as a consequence of the different environments that exist in organisations is the major reason why organisations need to look at the environment when formulating IS (Singh & Phil, 2012). This led to the following research proposition.

Proposition P4: *The macroenvironment is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

The next section discusses organisational governance as one key member trait influencing the behavioural intention to comply with the set IS parameters.

10.2 | Governance

Organisational governance is another key component identified as having an effect on ISC. IS management theorists assert that employee behaviour needs to be directed and censored to ensure amenability to organisational IS standards (Dhillon, Syed, & de Soares, 2015; Rastogi, & Von Solms 2012; Vroom & Von Solms, 2004).

An ISC in the banking sector is a prerequisite for good governance and the application of an effective regulatory framework (Da Veiga & Martins, 2014). However, 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 (Vignesh & Asha, 2015). Governance needs to be reinforced to ensure the functional integration of the systems and structures (Kufandirimbwa, Zanamwe, Hapanyengwi, & Kabanda, 2013). In the context of BYOD for banks, a good governance system will improve IS, thereby forming an ISC for the BYOD unintended administrator. The literature identified governance as a key function in the formulation of the behavioural intention to observe IS. Koh, Ruighaver, Maynard, and Ahmad (2005) propose a model that assumes that governance influences the ISC. The following research proposition was therefore formulated.

Proposition P5: *Governance is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

10.3 | Training

Training on the organisation's IS plan is another key component that was identified from the literature review as a pillar in building ISC. Employees come from different backgrounds, which means that most of them lack basic awareness of the consequences of breaching IS guidelines (Al-shehri, 2012). IS training differs from awareness in that training is more formal and confined to classrooms, whereas awareness is more relaxed and highly informational (Lim, Ahmad, Chang, & Maynard, 2010). Training teaches employees to be conscious of the ISC in their organisation, while awareness conscientises them. Further, organisations might not achieve high levels of IS if training is low among employees (Lim et al., 2010).

Banks thus need to ensure that their employees are aware of the organisational IS standards. This can be achieved through awareness campaigns, bulletins, and other available means to reach employees. A number of researchers believe that there is need for a continuous IS training programme to ensure initial education, and regular updates and reminders should reach the employees (Gundu & Flowerday, 2013; Von Solms & Von Solms, 2001). On the same construct of training, Brodin (2016a) states that information training is an area that requires improvement in many organisations. Organisations have to take proactive measures to make sure that their employees are aware of the organisational direction and position regarding IS (Brodin, 2016b). Therefore, because this paper views training as a significant trait for the existence of a positive behavioural intention towards IS, the following research proposition has been formulated.

Proposition P6: *Training is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

11 | ANALYSIS AND FINDINGS

In this section, the findings of the literature review and the survey results are analysed and presented. These are then used to evaluate the propositions made on the six traits identified as important in developing a behavioural intention to build a BYOD ISC. The results of the evaluation of propositions are used to quantify the model constructs as shown in Figure 1. An evaluation of the theoretical propositions has been rigorously conducted. This was achieved through a statistical analysis of the survey results. The findings were then added to the model for building an ISC for the BYOD unintended administrator.

The next section covers the proposed model and the statistical analysis of the survey results.

11.1 | The proposed model

Figure 1 illustrates the combination of individual and organisational traits culminating in a BYOD BISB model for the banking sector in Zimbabwe. In the model, the individual and organisational traits complement each other as constructs. The traits were amalgamated from the literature study

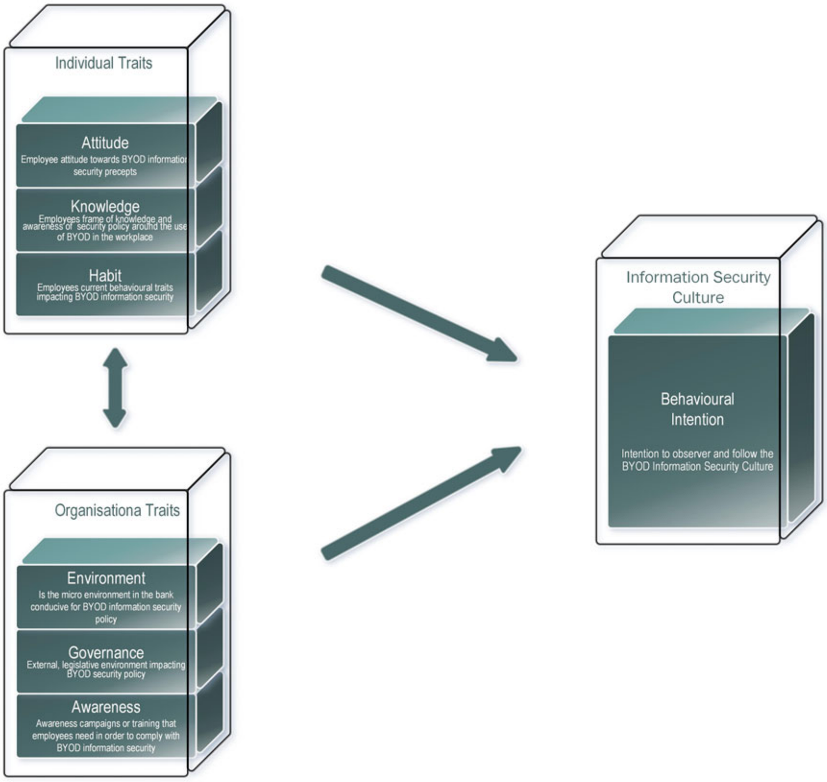
Individual Traits
Attitude
Employee attitude towards BYOD information security precepts
Knowledge
Employees frame of knowledge and awareness of security policy around the use of BYOD in the workplace
Habit
Employees current behavioural traits impacting BYOD information security
Organisationa Traits
Environment
Is the micro environment in the bank conducive for BYOD information security policy
Governance
External, legislative environment impacting BYOD security policy
Awareness
Awareness campaigns or training that employees need in order to comply with BYOD information security
Information Security Culture
Behavioural Intention
Intention to observer and follow the BYOD Information Security Culture

FIGURE 1 The proposed bring your own device (BYOD) information security behavioural (BISB) model

and funnelled into the behavioural intention construct, which represents the BISB. The BISB model will be tested to confirm its applicability. This will follow the analysis and findings of the results.

The next section contains the tests that were conducted on the constructs of the proposed model. This is followed by the final version of model, which is a culmination of the results from the tests conducted and the outcomes of the literature review.

11.2 | Correlation between variables

A perfect positive linear relationship or correlations between the variables are shown by a Pearson correlation of +1 points, while a Pearson value of 0 indicates an uncorrelated relationship between the variables.

From the results of the correlation coefficients contained in Table 2, the behavioural intention is positively related to five of the six model constructs of attitude, governance, training, environment, and knowledge, with the strongest positive relationship existing with governance followed by attitude, giving 0.327 and 0.32 values, respectively. There is an inverse correlation between habit and behavioural intention. The correlation results contained in Table 2 will be used to evaluate the propositions.

11.3 | Regression analysis

From the output presented in Table 3, it can be concluded that behavioural intention depends on the individual and organisational traits, which collectively explain 32.1% (R^2 = 0.321) of the total output control.

The other predictive variables of attitude (0.123), knowledge (0.630), environment (0.127), governance (0.176), and training (0.381) affected the dependent variable.

The beta weight habit (Habit = −0.059 at $P > 0.05$) showed a negative effect on the dependent variable. Regression analysis was used to test the relationships between the dependent variable and the independent variables. A significance level of $P < 0.05$ was chosen for this analysis, and the criteria for multicollinearity were set at a tolerance value of more than 0.25. While the other two variables (habit and knowledge) showed positive results that were not necessarily significant at $P < 0.01$, the resultant statistics combined with the supporting evidence from the literature review confirm their relevance in explaining behavioural intention.

The next section contains the evaluation of the research propositions, which form the model.

11.4 | Evaluation of propositions

Table 4 contains a summary of the Cronbach's alpha coefficient, R^2, and the beta values of the theoretical proposition evaluation. The statistical propositions individually contribute to the subjective probability that IS should be treated as a culture in the context of BYOD IS.

Proposition P1: *Employee attitude towards IS is positively associated with building an ISC for the BYOD unintended administrator.*

TABLE 2 Variable correlations

Scale	BI	ATT	KNO	HAB	ENV	GOV	TRA
Behavioural intention (BI)	-	0.32**	0.11	−0.59	0.262**	0.327**	0.27**
Attitude (ATT)		-	0.11	−0.59	0.262**	0.327**	0.270**
Knowledge (KNO)			-	−0.14	0.18*	0.04	0.19*
Habit (HAB)				-	0.045	0.185*	0.24**
Environment (ENV)					-	0.350**	0.38**
Governance (GOV)						-	0.24**
Training (TRA)							-

*Correlation is significant at the 0.05 level (2-tailed).

**Correlation is significant at the 0.01 level (2-tailed).

TABLE 3 Regression analysis summary

	Independent variable	Coefficient	Beta	R^2	*F*	Sig
Behavioural Intention	Attitude	0.47	0.123	0.32	9.4	0.142
	Knowledge	−0.46	0.630			0.630
	Habit	−0.77	−0.059			0.472
	Environment	0.086	0.127			0.143
	Governance	0.201	0.176			0.041
	Training	0.434	0.381			0.000

TABLE 4 Evaluation of research propositions

Proposition	Cronbach's Alpha Coefficient	R^2 Value	Beta Value	Result
P1 (Attitude)	0.719	0.321	0.127	Accepted
P2 (Knowledge)	0.390	−0.59	−0.059	Rejected
P3 (Habit)	0.320	0.108	−0.46	Rejected
P4 (Environment)	0.720	0.270	0.381	Accepted
P5 (Governance)	0.800	0.262	0.127	Accepted
P6 (Training)	0.600	0.327	0.176	Accepted

On the basis of the statistical computations contained in Table 4, attitude loaded positively in all the computations, with a Cronbach's alpha coefficient value of 0.719, confirming that it is a valid construct for the model. Attitude also showed a strong positive correlation with behavioural intention with a value of 0.317. The multiple regression analysis, which had an R^2 value of 0.321, statistically showed that attitude is positively correlated to behavioural intention. Overall, attitude had a beta value of 0.127, which was sufficient to explain that it is a valid construct. In combining the results of these statistical computations, Proposition P1 can be confirmed as positive, indicating that employee attitude is indeed important in building an ISC for the BYOD unintended administrator.

Proposition P2: *Employee knowledge is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

From Table 4, knowledge loaded with a Cronbach's alpha coefficient value of 0.390, which is deemed statistically invalid. The results of the correlation computation R^2 between knowledge and behavioural intention yielded a negative value of −0.59. Statistically, it shows a negative relationship between knowledge and behavioural intention, and it is not significant enough to have the requisite statistical effect. The multiple regression beta value for regression showed a negative value of −0.059, which indicates that there is an inverse relationship between knowledge and behavioural intention. In the context of this proposition, the relationship means that the more the employees know about the BYOD IS, the less likely they are to show a behavioural intention for building an ISC. Therefore, this neither confirms nor invalidates Proposition P2.

Proposition P3: *The employee's habits towards IS are positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

Statistical results in Table 4 on the habit construct loaded negatively on all the conducted tests. The Cronbach's alpha coefficient result from habit indicated a value of 0.320, which is deemed invalid. The correlation coefficient R^2 results between habit and the dependent variable of behavioural intention showed a negative value of 0.108, implying that there is a weak positive relationship between habit and behavioural intention. The multiple regression computations also loaded a −0.46 beta value, indicating that the relationship is inverse. From the 32.1% that the constructs explain in the relationship between the dependent and independent variables contained in Table 3, it can be concluded that that habit does not contribute positively. Statistically, it cannot be concluded that habit positively affects behavioural intention, and therefore, Proposition P3 was not confirmed statistically.

Proposition P4: *The environment is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

From Table 4 results, the environment as a construct evaluated under Proposition P4 loaded positively with a Cronbach's alpha coefficient of 0.720, indicating strong validity. The correlation coefficient R^2 between environment and behavioural intention loaded positively with 0.270, indicating a strong positive correlation. The regression beta value was 0.381. These statistical calculations confirm that indeed, Proposition P4 is valid.

Proposition P5: *Governance is positively associated with building an ISC in the BYOD phenomenon in a commercial bank in Zimbabwe.*

The Cronbach's alpha value for governance as contained in Table 4 loaded at 0.800, confirming validity, followed by a correlation coefficient R^2 value of 0.262 and a regression value of 0.127, which all confirmed a positive relationship between behavioural intentions as a dependent variable and governance. These statistics individually confirm Proposition P5 and collectively validates the model construct of governance.

Proposition P6: *The training organisations offer to employees is positively associated with building an ISC in the BYOD phenomenon.*

In Table 4, Cronbach's alpha coefficient for training loaded significantly at a value of 0.600, indicating that training positively influences the behavioural intention construct. The correlation coefficient R^2 between training and behavioural intention loaded with a significant value of 0.327, indicating a strong correlation. The regression coefficient of 0.327 indicated the highest correlation, confirming that indeed, Proposition P6 is valid.

The propositions above each contribute to the subjective probability that IS should be treated as a culture when addressing BYOD security. Table 4 provides a summary of the statistics used to evaluate the theoretical propositions.

The beta weight habit (Habit = −0.46 at $P > 0.05$) and knowledge (Knowledge = −0.059 at $P > 0.05$) showed a negative effect on the dependent variable as forming the basis of the rejection shown in Table 4.

From the evaluation of the propositions above, Propositions P1, P4, P5, and P6 were found to be statistically positive and were accepted in explaining the behavioural intention to build an ISC based on the *P*-values. Propositions P2 and P3 showed unacceptable and negative statistical results, indicating that they did not statistically explain the model based on the survey conducted. Regression analysis was used to test the relationships between the dependent variable and the independent variables.

While Propositions P2 and P3 were rejected statistically, the results obtained from the literature were deemed sufficient, and the propositions were therefore retained as constructs of the model until further testing can be done. Regarding P2 (knowledge), Twinomurinzi and Mawela (2014) point out that knowledge is in essence the operational knowledge of the technical devices used and how it fits in the organisation's security policy framework. They further argue that operational knowledge of the devices ensures secure use of the device; for instance, employees will need operational knowledge to understand the risks of downloading software that may be malicious to their operations (Twinomurinzi & Mawela, 2014). Ahmed and Sundaram (2011) argue that knowledge underpins the success of knowledge management initiatives in an organisation and has been recognised as vital for organisational transformation and success in implementing new solutions and standards in the business.

With regard to P3 (habit), social theorists agree that people act habitually in the world, not reflectively (Hopf, 2010). Employees develop certain routines when dealing with information assets, which collectively influence habitual perceptions that inform ways the OISC of an organisation can be improved. Therefore, organisations should consider employees' habits when dealing with BYOD IS (Chen et al., 2015).

Attitude, environment, governance, and training, as shown in Table 4, all displayed valid Cronbach's alpha, R^2, and beta values, whereas values related to attitude and knowledge were invalid. Nevertheless, as stated above, these two constructs were still retained as valid model constructs. The BISB model is designed to qualitatively present the components required for building an ISC for the BYOD unintended administrator. Qualitative research helps researchers to understand people in social and cultural contexts in which they exist. Quantitative research often fails to account for the social and institutional context that is generally retained when qualitative data is used (Myers & Avison, 2002). All six model constructs were therefore deemed valid in influencing the BISB for the unintended administrator.

The next section examines the BYOD BISB model constituting the findings for this paper.

12 | THE BISB MODEL

The six constructs were combined to build an ISC model. Figure 2 shows the final BISB model, which is a combination of the individual and organisational traits and the results from the statistical tests conducted. The various components were described in detail in Section 11. In the model, the individual and organisational traits complement each other as constructs for the BISB model. The literature review conducted confirms the contribution of the six propositions.

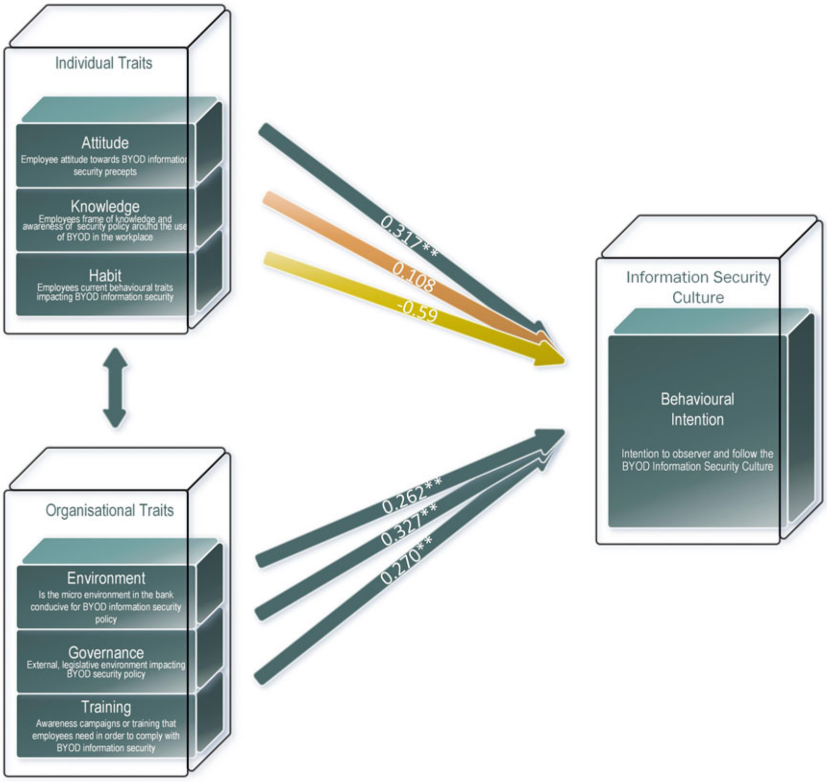
Individual Traits
Attitude
Employee attitude towards BYOD information security precepts
Knowledge
Employees frame of knowledge and awareness of security policy around the use of BYOD in the workplace
Habit
Employees current behavioural traits impacting BYOD information security
0.317**
0.108
-0.59
Information Security Culture
Behavioural Intention
Intention to observer and follow the BYOD Information Security Culture
Organisational Traits
Environment
Is the micro environment in the bank conducive for BYOD information security policy
Governance
External, legislative environment impacting BYOD security policy
Training
Awareness campaigns or training that employees need in order to comply with BYOD information security
0.262**
0.327**
0.270**

FIGURE 2 The bring your own device (BYOD) information security behavioural (BISB) model

With regard to Proposition P1, the attitude construct, Van Niekerk and Von Solms (2010) confirm that attitude determines the employee ISC because it influences the level at which they observe the policy frameworks and rules concerning its implementation. On a related perspective, Lee et al. (2016) state that employees' attitude to comply with the IS policies and standards in an organisation mitigates work overload and invasion of privacy, which they formulated into an IS stress management model.

In connection with Proposition P2, the knowledge construct of the BISB model, Alfawaz et al. (2010) propose IS behaviour in which knowledge is a key component. Mphahlele (2016) further contextualises this in banking by stating that operational knowledge of the organisational policy framework is central to implementing BYOD IS.

Proposition P3, employee habit, is a key BISB model construct. Vance et al. (2012) state that a behavioural intention is formulated from employees' unconscious or automatic behaviour, which is a routinised form of past behaviour.

Because the IT environment has changed as a result of the massive penetration of mobile devices such as smartphones, tablets, and phablets, this requires a conducive environment to curb the IS challenges that arise as a consequence of this change (Vignesh & Asha, 2015). This forms Proposition P4 of the BISB model. Farooq and Amin (2017) maintain that the environment determines the level of sophistication and the rate at which BYOD security is propagated.

The construct of governance, Proposition P5, is regarded by IS theorists as central to influencing behavioural intention to build an ISC. Dillon, Stahl, and Vossen (2015) argue that employee behaviour needs to be directed and censored to ensure that it is amenable to organisational IS standards. Vroom and Von Solms (2004) caution that there is urgent need for organisations, including banks, to modify their IS governance policies so as to address the challenges associated with BYOD.

In order to propagate all this, Al-shehri (2012) believes that training on the organisation's IS plan is another key component, which is a pillar of the behavioural intention to build an ISC. This is why Proposition P6, training, was deemed relevant as a construct of this model. To support this, Brodin (2016b) warns that organisations have to take proactive measures to make sure that their employees are aware of the organisational direction and position regarding IS so as to mitigate challenges.

The views of the various scholars on securing the BYOD problem as manifested in the BYOD unintended administrator suggest that behavioural intention can be achieved by harnessing the six BISB model constructs. The six constructs combined contribute to behavioural intention, which is a combination of individual and organisational traits. Notably, a combined effort by the organisation and its employees is required. Behavioural intention will result in a culture that in effect becomes the organisation's BYOD IS behavioural culture.

The next section evaluates the BISB model by means of an expert review process.

13 | EVALUATING THE BISB MODEL

There are several methods of evaluating research, including research symposiums, research consortiums, peer feedback, industry expert review, journals, and conferences (Ahmed & Sundaram, 2011). Considering that the BISB model is targeted at making it easier for bank chief information officers (CIOs) and security experts to manage IS, an expert review was selected as the most appropriate approach to evaluating the model. In an expert review process, an expert uses his or her knowledge and experience to give an expert judgement by identifying problems and recommending changes (Korhonen, Paavilainen, & Saarenpää, 2009). A questionnaire was framed and presented to 16 CIOs from banks in Zimbabwe. The profile for the selection criteria of respondents was centred on CIOs for banks in the Zimbabwean banking industry. The questions were designed to evaluate the model in terms of the seven-point evaluation criteria of completeness, consistency, accuracy, performance, usability, reliability, and best fit. The expert review approach was also considered to be an appropriate research evaluation method because the CIOs were the relevant available experts to provide the required input and the fact that they would be in a position to implement the BISB model in the event that their bank adopts it.

From the evaluation of the theoretical propositions used in formulating the BISB model, Table 2 shows that statistically, four of the model constructs are all significant. The statistically insignificant constructs were still retained because from the literature review, the findings built a strong case in support of them. Table 5 contains the questions and results of BISB evaluation questions grouped under each criterion of the seven-point classification.

The seven evaluation points presented to the CIOs during the expert review process all elicited positive feedback about the relevance of the BISB model. The CIOs' responses and feedback are presented in Figure 3 as percentages quantifying the degree of relevance to the various banks as a function of the total responses received.

The general trend analysis of the results obtained from the expert review shows the bank CIOs' acceptance of the BISB model. The CIOs all have more than 5 years of experience working in the Zimbabwe banking sector. The questions were designed to evaluate the model against the criteria of completeness, consistency, accuracy, performance, usability, reliability, and best fit. A considerable number agreed that the BISB model satisfies their requirements, with a small number neither agreeing nor disagreeing. Very few to none of the CIOs disagreed with the BISB model. On the measurement criterion, close to 70% of the CIOs agreed that the BISB model is a complete presentation of how the unintended administrator can be secured, while above 15% completely agreed with the model. On consistency, more than 70% agreed, followed by above 20% who completely agreed. On the accuracy criterion, 50% agreed with the model, and 35% completely agreed. Computations from the performance measurement criterion show above 65% agreed with the BISB model, and about 18% completely agreed. On usability as a criterion, about 50% agreed,

TABLE 5 Bring your own device (BYOD) information security behavioural (BISB) model evaluation criteria

Completeness	Not exhaustive	To a lesser extent	Moderately exhaustive	To a larger extent	Completely exhaustive
To what extent are the BISB individual traits exhaustive in covering the employee's contribution to information security in the BYOD?	0	0	4	9	3
To what extent are the BISB organisational traits exhaustive in covering the employee's contribution to information security in the BYOD?	0	0	2	12	2
Consistency	Completely disagree	Disagree	Neither agree nor disagree	Agree	Completely agree
Do you feel that the BISB model will maintain its relevance with the ever-changing security landscape?	0	1	1	8	6
How well structured are the arguments for the BISB model?	0	0	0	14	2
Accuracy	Very inaccurately	Inaccurately	Moderately	Fairly accurately	Very accurately
How accurately do you think the BISB model addresses the challenges of information security around BYOD in Zimbabwe?	0	0	2	8	6
How comprehensive is the BISB model in addressing the factors affecting information security around BYOD?	0	0	0	10	6
Performance	Extremely unlikely	Unlikely	Indifferent	Likely	Extremely likely
How likely are you to recommend that your organisation adopt the BISB model?	0	0	1	10	4
How likely is your organisation to adopt the BISB model on your recommendation?	0	2	2	10	2
Usability	Very inapplicable	Inapplicable	Moderately applicable	Fairly applicable	Very applicable
How applicable is this model to your organisation?	0	0	3	9	4
How adaptable is the BISB model to the various banks in Zimbabwe?	0	2	1	7	6
How applicable is this model in Zimbabwe's banking environment?	0	0	2	9	5
Reliability	Completely disagree	Mostly disagree	Agree on some aspects	Mostly in agreement	Completely in agreement
How much of the model are you in agreement with?	0	0	3	11	2
How much of the BISB model is already in practice in your organisation?	1	2	2	10	1
Best Fit	Does not fit	To a lesser extent	Indifferent	To a larger extent	Seamlessly
To what extent does the BISB model fit in with the existing security culture at your organisation?	1	0	0	13	2
How easily can the BISB model be applied to your organisation?	0	4	0	9	3

while about 35% were completely in agreement. Reliability as a criterion displayed agreement of above 65%, while 15% completely agreed. On the best fit criterion, about 70% agreed, followed by 15% completely in agreement. Across all seven measurement criteria, a summation of the results from the scale measurement of agree and completely agree was found to be above 50%. This response confirms that there is a general positive evaluation of the BISB model.

While IS is viewed as a preserve of the banks' IT department, the CIOs agreed on the need for all the departments to take ownership of IS management. According to the seven evaluation criteria used in the evaluation process, the results strongly indicate how important the unintended administrator has become in the BYOD era. The experts' feedback also highlights the importance of including the BISB model in organisational strategy. Some participants in the review process suggested that the BISB model be included in the new employee onboarding process. They believe that the best way to build a behavioural intention that advocates IS is to educate them before they become full members of the organisation. Other experts believe that organisations' vision and mission statements should reflect the organisational appetite for IS, especially by including the BISB model components. Some experts were of the view that posters and charts be made available to employees so that the BISM model becomes a living document.

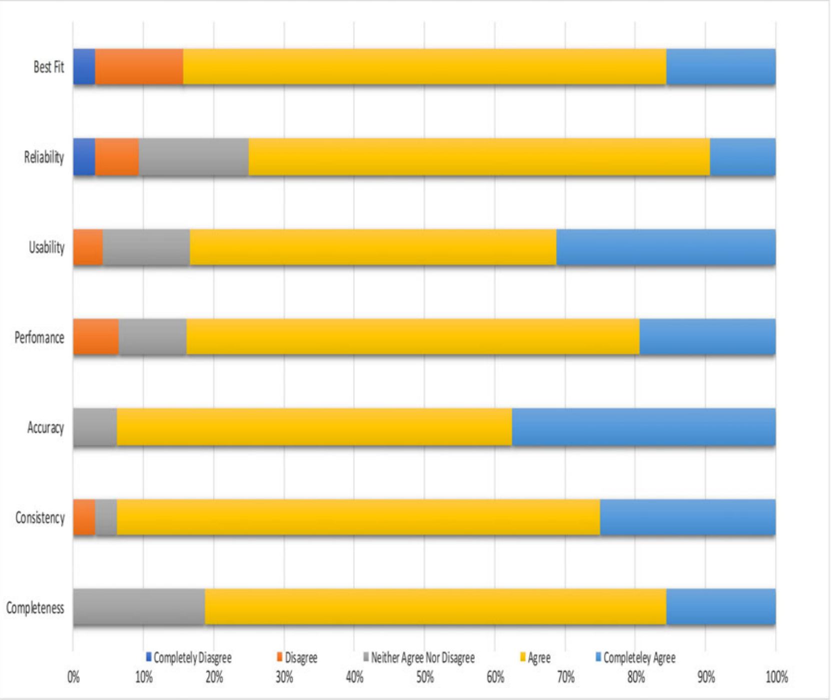

FIGURE 3 Expert review results

14 | LIMITATIONS AND FUTURE WORK

The banking sector in Zimbabwe consists of locally owned and foreign-owned banks. This study is, however, limited to a case study conducted at one commercial bank in Zimbabwe. This may imply that the model constructs are not necessarily exhaustive. Future research could cover a wider spectrum of banks in Zimbabwe. Future work will also include more than one bank, and further tests will be conducted on the results so as to make wider statistical inference, which will help in making a more informed model evaluation. Additional constructs will also be considered for the BISB model.

15 | CONCLUSION

The purpose of this paper is to show how banks can mitigate IS risks caused by the unintended administrator using the BYOD BISB model. This paper discusses how banks can build an ISC for the BYOD unintended administrator and provides an overview of how BYOD has affected the way IS is being managed in organisations. The paper indicates how employees who own such devices have become unintended administrators in the BYOD phenomenon and thus introduce security risks; the identification of individual and organisational traits formed the constructs for the BYOD BISB model, which was tested via the statistical survey.

The relevance and applicability of the model is determined by the effect it will have in enabling banks to secure the unintended administrator in a BYOD environment. It was noted that the BISB model will quicken banks' pace to catch up with BYOD security. Overall, the model was regarded as applicable in building an ISC for banks in Zimbabwe. It can be inferred that the solution to securing the BYOD unintended administrator lies within the unintended administrator. BYOD IS can therefore be viewed as a combination of the individual traits of the employees and the traits of the organisation for which they work.

ORCID

Alfred Musarurwa https://orcid.org/0000-0002-5455-0871
Stephen Flowerday https://orcid.org/0000-0002-4591-3802
Liezel Cilliers https://orcid.org/0000-0001-9493-4311

REFERENCES

Ahmed, G., Ragsdell, G., & Olphert, W. (2014). *Knowledge sharing and information security: A paradox?* (pp. 132–146). Academic Conferences and Publishing International Limited: Berlin, Germany.

Ahmed, M. D., & Sundaram, D. (2011). Design science research methodology: An artefact-centric creation and evaluation approach. ACIS 2011 proceedings.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: A behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security*-Volume 105 (pp. 47–55). Australian Computer Society, Inc.: Brisbane, Australia.

AlHogail, A., & Mirza, A. (2015, January). Organizational information security culture assessment. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp): Las Vegas, USA.

Allam, S., Flowerday, S., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*, 55–65.

Al-shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences*, *6*(1), 61–69.

Arregui, D., Maynard, S., & Ahmad, A. (2016). Mitigating BYOD information security risks. *Australasian Conference on Information Systems*, *2016*, 1–11.

Bransford, J. (2000). *How people learn. Brain, mind, experience, and school (expanded)*. Washington DC: National Academies Press, 5(1) 77–96.

Betz, L. (2016). An analysis of the relationship between security information technology enhancements and computer security breaches and incidents.

Brodin, M., (2016a), 'BYOD vs. CYOD—What is the difference?', in M.B. Nunes, P. Isaías & P. Powell (eds.), *IADIS international conference information systems*, vol. 3, pp. 55–62, Vilamoura, Portugal: IADIS Press, December 11–14, 2016. P. Powell (Eds.).

Brodin, M. (2016b). Management of mobile devices: How to implement a new strategy. In The 27th International Business Information Management ge sharing and information seAssociation Conference, IBIMA 2016, Milan, Italy, (1261–1268).

Cameron, C. (2012). *The BYOD security challenge: How scary is the iPad, tablet, smartphone surge?* Eset: Michigan, USA.

Chen, H., Li, J., Hoang, T., & Lou, X. (2013). Security challenges of BYOD: A security education, training and awareness perspective. Unpublished, 1–8.

Chen, J. (2014). Enterprise mobility: The next major risk management challenge. (cover story). *Directors & Boards*, *39*(1), 18–21.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19.

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

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207.

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., Syed, R., & de Soares, F. (2015). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *ge sharing and information seInformation and Management*, *32*(1), 40–74.

Dillon, S., Stahl, F., & Vossen, G. (2015). BYOD and governance of the personal cloud. *International Journal of Cloud Applications and Computing*, *5*(2), 23–35.

Eschelbeck, G., & Schwartzberg, D. (2012). BYOD risks and rewards: How to keep employee smartphones, laptops and tablets secure. A Sophos Whitepaper 06. 12v1.dNA. Boston, USA.

Farooq, O., & Amin, A. (2017). National culture, information environment, and sensitivity of investment to stock prices: Evidence from emerging markets. *Research in International Business and Finance*, *39*(3), 41–46.

Frauenstein, E. D., & Flowerday, S. V. (2016, August). Social network phishing: Becoming habituated to clicks and ignorant to threats?. In *Information Security for South Africa (ISSA)*, 2016 (pp. 98–105). IEEE.

Garba, A., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security*, *11*(1), 38–54.

Ginovsky, J. (2012). "BYOD". American Bankers Association. *ABA Banking Journal*, *104*(4), 24.

Gundu, T., & Flowerday, S. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69–79.

Gustav, A., & Kabanda, S. (2016). BYOD adoption concerns in the South African financial institution sector. In *In AIS 2016 proceedings (CONF-IRM)*. Cape Town: International Conference on Information Resources.

Haworth. (2015). How to create a successful organizational culture: Build it—literally? Michigan, USA.

Hopf, T. (2010). The logic of habit in international relations. *European Journal of International Relations*, *16*(4), 539–561.

Keyes, J. (2013). *Bring your own devices (BYOD) survival guide*. Boston, USA: Taylor & Francis.

Koffer, S., & Fielt, E. (2015). IT consumerization and its effects on IT business value, IT capabilities, and the IT function. *PACIS 2015 Proceedings*, *3*(2), 17.

Köffer, S., Fielt, E., & Niehaves, B. (2015). IT consumerization and its effects on IT business value, IT capabilities, and the IT function. In *PACIS 2015 Proceedings: Pacific Asia Conference on Information Systems*. The Association for Information Systems (AIS).

Koh, K., Ruighaver, A., Maynard, S., & Ahmad, A. (2005, September). Security governance: Its impact on security culture. In AISM (47–58).

Korhonen, H., Paavilainen, J., & Saarenpää, H. (2009). Expert review method in game evaluations: Comparison of two playability heuristic sets. *MindTrek*, *2009*(January), 74–81.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296.

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.

Lanaj, K., Johnson, R., & Barnes, C. (2014). Beginning the workday yet already depleted? Consequences of late-night smartphone use and sleep. *Organizational Behavior and Human Decision Processes*, *124*(1), 11–23.

Leclercg-Vandelannoitte, A. (2015). Information technology & people article information: Information technology & people, 28(1), 2–33.

Lee, C., Lee, C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security*, *59*, 60–70.

Lennon, R. G. (2012, October). Bring your own device (BYOD) with cloud 4 education. In *Proceedings of the 3rd annual conference on Systems, programming, and applications: Software for humanity* (pp. 171–180). ACM.

Lim, C., & Churchill, D. (2016). Mobile learning. *Interactive Learning Environments*, *24*(2), 273–276.

Lim, J., Ahmad, A., Chang, S., & Maynard, S. (2010, July). Embedding information security culture emerging concerns and challenges. In *PACIS* (p. 43).

Lundy, O., & Cowling, A. (1996). Strategic human resource management. In *London Routledge* (6th ed.). London: London: Routledge.

Mohanty, A. (2015). Effective team building, organisational culture and organisational climate in service sector—A study with special reference to hotels in Odisha Ashish Mohanty. *International Journal of English Language, Literature and Humanities*, *3*(7), 499–516.

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8.

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

Myers, M., & Avison, D. (2002). Qualitative research in information systems. *Management Information Systems*, *21*(2), 241–242.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In System sciences, 2007. HICSS 2007. 40th annual Hawaii International Conference on (156b). IEEE.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015). Examining attitudes toward information security behaviour using mixed methods. In HAISA (57–70).

Peslak, A., Ceccucci, W., & Sendall, P. (2012). An empirical study of social networking behaviour using theory of reasoned action. *Journal of Information Systems Applied Research*, *5*(3), 12.

Puhakainen, P., & Siponen, M. (2010). Improving employee' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778.

Rastogi, R., & Von Solms, R. (2012). Information security service culture—Information security for end-users. *Journal of Universal Computer Science*, *18*(12), 1628–1642.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78.

Safa, S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13.

Schein, E. (2009). *The corporate culture survival guide. John Wiley Trade (New and Re, Vol. 1)*. San Francisco, California: Jossey Bass a Wiley Imprint.

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

Shumate, T., & Ketel, M. (2014, March). Bring your own device: Benefits, risks and control techniques. In *Southeastcon 2014*, (1–6). IEEE: Lexington, Kentucky.

Singh, M., & Phil, M. (2012). B.Y.O.D. genie is out of the bottle—“Devil or Angel”. *Journal of Business Management & Social Sciences Research*, *1*(3), 1–12.

Von Solms, B., & Von Solms, R. (2001). Incremental information security certification. *Computers and Security*, *1*(5), 14–35.

Stewart, J., Chapple, M., & Gibson, D. (2012). *CISSP: Certified Information Systems Security Professional study guide*. John Wiley & Sons: Indiana, USA.

Tharp, B. (2009). Defining “Culture” and “Organizational Culture”: From anthropology to the office. *Interpretation a Journal of Bible and Theology*, *2*(3), 1–5.

Twinomurinzi, H., & Mawela, T. (2014, September). Employee perceptions of BYOD in South Africa: Employers are turning a blind eye? In Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology (126). ACM.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476–486.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information and Management*, *49*(3–4), 190–198.

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science*, *50*, 511–516.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198.

Wood, C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud and Security*, *2004*(1), 16–17.

AUTHOR BIOGRAPHIES

Alfred Musarurwa is currently the Chief Information Officer (CIO) of Nedbank Zimbabwe. Alfred holds a PhD degree in Information Systems from the University of Fort Hare. He also holds MSc and BSc degrees in Computer Science and Statistics from the University of Zimbabwe. Alfred is also a certified Information security specialist as well as a certified ethical hacker. He has experience in ICT spanning 15 years in the financial services sector with experience ranging from software development, project management, information security management, as well as network administration and management. He has written published conference and journal papers around information security as well as the enterprise mobility.

Stephen Flowerday holds a BSc and an MBA, as well as a doctoral degree (IT). He is a full professor and Head of Department at Rhodes University and an adjunct professor at the University of Fort Hare. He is a reviewer for conference publications, a guest editor and reviewer for a number of academic journals, and serves on various panels of the National Research Foundation (NRF). His research focus area is behavioural cybersecurity.

Liezel Cilliers is a senior lecturer in the Department of Information Systems at the University of Fort Hare. She completed a DPhil (Information Systems) in 2014. In 2016, she was awarded the Vice Chancellor's Excellence award in the category of experienced Teacher, while she received the Vice Chancellor's Excellence award in the category emerging Researcher in 2015. Her research areas include technology in education and e-health.

How to cite this article: Musarurwa A, Flowerday S, Cilliers L. The bring-your-own-device unintended administrator: A perspective from Zimbabwe. *E J Info Sys Dev Countries*. 2019;e12076. https://doi.org/10.1002/isd2.12076

APPENDIX 1: RESEARCH INSTRUMENT

Questionnaire: A Model for Building an Information Security Culture for the Bring Your Own Device: the case of the unintended administrator

Section 1: Demographics

1. What is your gender?
   - Male
   - Female
2. Indicate your age.
   - < 30 years
   - 30-40 years
   - 41-50 years
   - > 50 years
3. How long have you been employed?
   - <5 years
   - 5-10 years
   - 11-15 years
   - > 15 years
4. The information that I deal with:
   - Is extremely confidential (where confidentiality is enforced by the RBZ)
   - Has sensitive details about internal operations of the bank.
   - Is sensitive but mostly functional.
   - General and not damaging to the bank.
5. Which of the following devices do you own?
   - Smartphone
   - Tablet
   - Laptop
   - Desktop
   - USB/Flash drive
   - Hard Disk Drive/External Hard Drive
6. Are you accessing any of the following services from your personal device? (Select one or more options).
   - Access email
   - Make work related phone calls
   - Access the company's non-banking systems
   - Access the company's banking systems
   - Work calendar

Knowledge-I am knowledgeable of the following regarding the use of BYOD in my work place:

7.	Using a personal device at work would allow me access to all the information I require in order to perform my job satisfactorily.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
8.	Using personal devices to perform my tasks at work will not affect the quality of my work or how I interact with customers or colleagues.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
9.	There is a growing demand from employees for the use of personal devices in the banking environment to allow unmonitored access to information and systems.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
10.	Banks that allow employees to bring their own devices are more information security conscious than those that do not.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
11.	Technological innovation must be in the bank's objectives in order for BYOD to be successfully ingrained into company culture.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
12.	I understand the distinction between personal and organisational data and am able to keep them separate while using a personal device for work				YES	NO
13.	I think that the nature of my industry is such that the information is too sensitive to allow employees to bring and use their own devices for company business.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Attitude					
14.	I am willing to use my personal devices such as a smartphone and tablet to conduct the bank's business.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
15.	I feel that using my own devices in the workplace compromises my privacy.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
16.	I will only use my personal devices for work related business where there is a reimbursement policy.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
17.	Being cognisant of the sensitive nature of a bank's information and systems, I believe that if managed well, the advantages of BYOD outweigh the risks in today's modern technological era.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
18.	Do you believe that personal devices are being optimally managed within your bank in order to maximise their benefits while mitigating the information security risks?	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
19.	I believe that allowing bank employees to bring and use personal devices in the workplace is more beneficial than detrimental to their productivity.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
20.	I believe allowing employees to bring their own devices will create a more conducive working environment.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
21.	In light of the nature of my work and industry, the organisation should be able to monitor what I do on my personal device while in the work environment.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

(Continued)

22.	I am more comfortable in an environment where I am allowed to access some information such as email from a personal device than where I am not.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Habit					
23.	Are you currently allowed to use personal devices in the work environment for company business?			Yes	No	I don't know
24.	My personal devices are used by family, friends and colleagues when I am at home.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
25.	Personal and organisational data such as documents and contacts are stored together (are allowed to mix) on my personal devices that I use for work.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
26.	My personal devices that I use at work are secured by a password or PIN to ensure that both the company and my data is protected.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
27.	If my personal devices are stolen, I have contingency plans in place to ensure that my data does not fall into the wrong hands such as encryption, remote erase or remote disable.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Training					
28.	Have you ever received training around information security from your employer?				Yes	No
29.	If you answered yes to question 28 above, did that training involve aspects of information security around BYOD?				Yes	No
30.	I believe that training is the best way to communicate information security tenets of BYOD to ensure that they are understood and accepted as opposed to using fines, threat of punishment or other coercive methods.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
31.	There is need for education in order for employees to understand information security for the successful implementation of BYOD within my organisation.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
32.	I do not fully understand data ownership policies as defined by my bank such as distinctions between organisational and personal email, social network access and account ownership and business vs. personal contacts and need to be trained in these aspects.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
33.	I need to be taught how to access organisational resources from BYOD devices such as email and Customer Relationship Management (CRM) systems even where I am already familiar with these systems/resources in the work environment.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
34.	I could benefit from additional training on information security if my organisation wants to adopt BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Environment					
35.	The environment at my workplace is conducive to bring and use my personal devices (Considering such things as Internet connectivity and accessing networked resources).	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

(Continued)

36.	The technologies and applications I use at work are compatible with my personal devices.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
37.	The organisational culture at my place of work is not prohibitive to new technological trends such as BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
38.	My superiors are comfortable enough with technology to appreciate the benefits of BYOD?	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
39.	My company's information security policy is supportive of BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
40.	The information security culture in my organisation is robust enough to enable BYOD to be implemented successfully without infringing on information security policy.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
41.	Using my personal device for work will not create a risk of sensitive information leaking to outsiders.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Governance					
42.	There is need for the regulator to examine the implementation of and to have oversight over BYOD in the banking industry.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
43.	Information security policy around BYOD is best governed by placing the responsibility in the hands of the employees and only establishing controls.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
44.	Accountability for the information security around BYOD must lie with the risk department and not the IT department for BYOD to be managed successfully.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
45.	Legislation around data protection in the finance industry in Zimbabwe is robust enough to mitigate the new risks introduced by BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
46.	The Data Protection Bill support privacy on one's mobile device and can be a hindrance to the successful implementation of BYOD in Zimbabwe.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Behavioural intention					
47.	I am willing to participate in any activities organised by the bank in order to improve information security around BYOD such as workshops and focus groups.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
48.	I intend to comply with the bank's information security policies when using my own device for work purposes.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
49.	I am willing to use additional security measures at the bank's recommendation such as desisting from connecting my personal devices to unsecured public Wi-Fi access points or installing certain applications on devices that I use at work.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
50.	I am willing to invest money in more security measures for my personal devices that I will use at work.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
51.	I am willing to report any potential breaches of organisational data on	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

(Continued)

my personal devices even when I
do not think they pose a risk.

52. Please state below any other comments regarding BYOD policies in your bank.