South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

An information security behavioural model for the bring-your-own-device trend

Authors:
Alfred Musarurwa[1]
Stephen Flowerday[1]
Liezel Cilliers[1]

Affiliations:
[1]Department of Information Systems, University of Fort Hare, South Africa

Corresponding author:
Liezel Cilliers,
liezelcilliers@yahoo.com

Dates:
Received: 05 Mar. 2018
Accepted: 30 July 2018
Published: 05 Nov. 2018

How to cite this article:
Musarurwa, A., Flowerday, S. & Cilliers, L., 2018, 'An information security behavioural model for the bring-your-own-device trend', *South African Journal of Information Management* 20(1), a980. https://doi.org/10.4102/sajim.v20i1.980

Background: Organisations have found themselves in a race to embrace bringing your own device (BYOD) in their day-to-day business operations, while at the same time needing to maintain their information security management standards. BYOD is convenient for employees as it allows them to conduct business anywhere and at any time. However, this has resulted in organisations having to rethink their information security management, as BYOD now extends the information security management boundaries to wherever the employees takes their device and wherever there is a network access point.

Objective: While technical solutions are offered by various BYOD solution providers, the theme of this article is to propose employee behavioural change for organisations to mitigate the risks that are associated with the BYOD phenomenon.

Methods: For this purpose, a literature review was conducted, culminating in the identification of six key traits for the development of a behavioural intention model towards information security. Using the six traits, a questionnaire was developed and loaded on *SurveyMonkey*, and a survey was subsequently conducted among 270 employees of a selected bank in Zimbabwe.

Results: A total of 205 employees responded to the survey, with 179 of the responses being deemed usable (i.e. a response rate of 87%). Data obtained from the survey were subjected to statistical tests, the conclusions of which were used to create the BYOD information security behavioural (BISB) model.

Conclusion: The article concludes by proposing the BISB model as an effective option for mitigating the information security challenges in BYOD.

Introduction

Information security regarding bring your own device (BYOD) has become a point of focus for every organisation that is serious about security, as confirmed by Ackerman and Krupp (2012), who point out that BYOD has now become the rule rather than the exception in the modern workplace. This new form of information system implementation and management in the workplace has compelled organisations to change their information technology (IT) policies. Traditionally, responsibility for information security management in the workplace has been the preserve of a specialised IT department. However, as Musarurwa and Jazri (2015) argue, since 2010 there has been an exponential growth in Internet penetration in Africa, coupled with a massive influx of mobile smart devices. This has resulted in a net increase in mobile device penetration. A study conducted by FinScope (2014) found that there is a 100% mobile penetration in Zimbabwe, with some people owning more than one smartphone. This penetration level gives an indication that BYOD usage is prevalent in Zimbabwe. The same report also gave a comparative analysis to other African countries, where the majority of countries had a penetration rate of about 60% – 85%. The survey further found indications of growth in mobile penetration between 2010 and 2014.

Research by Vorakulpipat et al. (2017) identified a general shift from office-based work to ubiquitous office work, with employees now preferring to work on the move. This trend is extending office hours and giving employees the flexibility to work wherever they are. While most organisations have embraced the technology shift towards BYOD, Garza and Guo (2015) caution that most organisations that have embraced BYOD have found themselves playing catch-up when it comes to formulating policies that protect them against potential BYOD attacks. This seems to explain Larry Furst's (2013) comment that BYOD is in essence 'Bring Your Own Disaster', as information security exposure has increased as a result of BYOD proliferation. This article evaluates the information security behavioural (ISB) aspects of the employee that the organisation can use to mitigate the challenges that arise from BYOD.

This article addresses the way organisations can implement an ISB approach in helping to reduce the challenges presented by BYOD. The article takes the form of a literature review of the employees' impact on information security management in organisations. This is preceded by an overview of the information security practices that are implemented in organisations. The research methodology followed in this article took the form of a literature review followed by a single case study on a commercial bank in Zimbabwe. The research instrument was formulated from the literature survey and was consequently used to conduct a survey in the bank using an online questionnaire. Statistical analysis was conducted on the survey results, culminating in the identification of the traits of the model. The following sections give the theoretical foundation of the article. The ISB approach explored in this article will be the ultimate contribution of this article.

Theoretical foundation

This section presents the ISB traits, as well as some fundamental BYOD information security terminology that was harnessed in formulating the model.

Bring your own device in organisations

Cheng, Guan and Chau's (2016) findings place BYOD as a key competitive business trend that every organisation that is serious about remaining relevant should embrace. In applying BYOD, the administration removes responsibility for security from the IT department and places it in the hands of employees, who inadvertently become the 'unintended administrators' of the devices they use. Researchers of modern trends in business technology have cited various reasons for the popularity of BYOD. Agudelo et al. (2015) argue that BYOD reduces the overall IT hardware spend as employees now buy their own devices. In addition, because BYOD enables employees to access their work anywhere and at any time, there is a net increase in productivity (De Las Cuevas et al. 2015). Employees also generally prefer to choose the devices they work with, which brings a level of gratification and satisfaction. Moreover, the turnaround time for critical business information sharing improves with BYOD, such that if any given organisation chooses agility as a key performance differentiator, BYOD becomes an important catalyst (Agudelo et al. 2015). However, these benefits are also accompanied by challenges, which are explored in the next section.

Information security challenges for bringing your own device

Inasmuch as BYOD holds benefits for organisations, Kaneshige (2012) believes that there is a need for chief information officers to reconsider the benefits of BYOD. From a productivity standpoint, it is argued that employees participating in BYOD spend much of their time on social media applications such as instant messaging, Skype, Hangouts, Facebook and WhatsApp, which are key productivity killers. He also points out that most devices that are used by employees in BYOD do not meet the standards provided in the organisation's information security policy. Moreover, employees involved in BYOD use cloud services such as Dropbox and Google Drive to store documents, which may result in some organisational documents being compromised (Sophos 2017). In light of this, the information security management of BYOD becomes the responsibility of the employees, who are the unintended administrators of the devices they use. The next section examines ways in which the BYOD unintended administrator can be secured so that organisations can leverage the benefits that come with BYOD.

Securing the bring-your-own-device unintended administrator

Considering that the devices used in BYOD are provided by different technology vendors, attempts have been made to secure BYOD at both the technical and application levels of these devices. Organisations have also implemented virtual private networks that will only allow connections with trusted organisational devices (Vorakulpipat et al. 2017). Inasmuch as these solutions and mechanisms exist, they only work in a situation where the user is aware of the existence of such capabilities and is also trained on how to use them. Mindful of the existence of these technical solutions, the focus of this article is on securing the organisation beyond the technical solutions that are implemented by the technology vendors. The article thus explores the way organisations can mitigate BYOD information security risks at the device user level. In this article, the device user is referred to as the 'unintended administrator', who is any other non-technical employee who makes use of personal devices in BYOD.

From the literature review, six key components were identified as central to implementing information security at the employee level. These components were viewed as independent traits that should exist in order for an employee to develop a behavioural intention towards information security.

Behavioural intention

Behavioural intention is viewed as the perceived prospect of, or subjective probability that, an individual will engage in a particular behaviour. Research conducted by Tharp (2009) has shown that large numbers of studies in psychology focus directly on the individual as the locus of behaviour. He further points out that the complex whole, which includes knowledge, belief, arts, morals, law, custom and any other capabilities and habits acquired by humans as members of society, forms behavioural intention. The theory of planned behaviour provides a reliable reference for understanding behaviour by introducing the specific components of attitude, subjective norms and perceived behavioural control that directly influence employees' behavioural intentions. In terms of the theory, Ajzen and Fishbein (1977) argue that a person's perceived, and not necessarily actual, behavioural control is a sufficient motivator for influencing behavioural intention.

Traits of proposed behavioural intention

Behavioural intention is formulated as a culmination of the traits exhibited by the employees. The following sections examine the six traits that were proposed for determining the behavioural intentions of employees when implementing BYOD information security. Three individual traits of attitude, knowledge and habit were identified together with three organisational traits of environment, governance and training. It is important to note that inasmuch as a person or an organisation can have more than three traits, the selected traits were deemed more relevant, based on the literature review findings, as well as the statistical test conducted.

Attitude

Attitude can be viewed as a settled way of thinking or feeling about something. Da Veiga and Martins (2015) point out that this is determined by a person's attitudes and beliefs with respect to the issue at hand. Alfawaz, Nelson and Mohannak (2010) propose behavioural intention modes that organisations should observe when attempting to influence employees' attitudes. Attitude drives the employee's intention to behave and react in a particular way, which explains why Lee, Lee and Kim (2016) remark that employee attitude to compliance with the information security policies and standards in an organisation mitigates work overload and invasion of privacy. They further point out that this can be formulated into an information security stress management model. In this study, attitude was thus identified as being a key member trait in formulating a BYOD information security behavioural (BISB) intention. The next section addresses knowledge, which is the second individual trait identified as important in the model formulation.

Knowledge

Skills acquired through experience or education about BYOD information security assist employees in operating devices in BYOD. In order for BYOD information security to be implemented, there is a need for organisations to invest in employee training on and awareness of the consequences of not managing information security on their devices properly. Safa et al. (2015) point out that knowledge plays an important role in the information security domain, owing to the positive effect it has on fostering employees' information security training. Knowledge of the information security risks makes it easy for organisations to implement attendant information security policies and encourage the sharing of best practices. Von Solms and Van Niekerk (2013), however, caution that a lack of information security knowledge on the part of employees is detrimental to organisations and that such organisations must invest in employee knowledge. Habit has also been identified as one of the key traits for building an ISB intention. The next section explores habit in detail.

Habit

Regular tendencies or practices that an individual develops and are usually hard to give up are viewed as representing habit in this article. Social theorists have agreed that people generally act habitually in the world, 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 employees develop in using BYOD are part of the three individual traits identified in the literature. Organisations should therefore consider the impact of employees' habits when dealing with BYOD information security (Cheng et al. 2016). Employees develop certain routines when dealing with information assets that collectively have an influence on habitual perceptions, which inform ways in which ISB in an organisation can be improved. This is even more important with BYOD, as employees will also develop habits or routines on their private devices at home that will extend to the workplace. How employees secure their private phone, regarding physical access or authorisation to access the phone at home, is unlikely to change when they enter the workplace. Accordingly, this study suggests that habitual behaviour explains the ISB of individuals in any organisation.

Environment

Surrounding factors that affect, and are distinct and specific to, an organisation are identified in this article as the microenvironment. This is one of the key role components in formulating employee behavioural intention (Gordon 2015). Research conducted by Farooq and Amin (2017) has shown that a positive environment, that values employee contributions, is characterised by an employee behavioural intention where the employee values and observes organisational policies and standards. Vignesh and Asha (2015) argue that the massive penetration of mobile devices, such as smartphones, tablets and phablets has changed the business environment. This highly dynamic environment is characterised by complex competitive practices, where an employee finds derivative values that correspond to institutionalising the way organisations conduct their business. BYOD is one such derivative value that gives employees the latitude to work flexibly (Köffer & Fielt 2015). The environment furthermore determines the level of sophistication, as well as the rate at which BYOD security is propagated. The second organisational trait identified in this study is governance.

Governance

In the context of BYOD for organisations, a good governance system will improve information security, thereby forming a positive behavioural intention for the BYOD unintended administrator. Organisational governance is another key trait identified as having an impact on the employee's behavioural intention to observe information security in BYOD. Information security management theorists assert that

employee behaviour needs to be guided, directed and censored to ensure that it is amenable to organisational information security standards (Dillon, Stahl & Vossen 2015; Rastogi & Solms 2012; Vroom & von Solms 2004). Vignesh and Asha (2015) caution that there is an urgent need for organisations to modify their information security governance policies so as to address the challenges that come with BYOD. Kufandirimbwa et al. (2013) consider governance to be a key organisational function that needs to be reinforced to ensure the functional integration of the systems and structures. The next section identifies training, which is the last of the six traits identified in the literature review.

Training

The third organisational trait of training on information security for the organisation is another attribute identified as being key to influencing the behavioural intention to support a BYOD information security culture. Employees come from different backgrounds; nevertheless most of them lack basic awareness of the consequences they face if found to be in breach of information security guidelines (Al-shehri 2012). Information security training differs from awareness in that training is more formal and is confined to classrooms, whereas awareness is more relaxed and very informational (Lim & Churchill 2016). Von Solms and Von Solms (2004) confirm that there is need for an ongoing information security training programme to ensure initial education, as well as for regular updates and reminders to reach the employees. On the same trait of training, Brodin (2016) cautions that information training is an area that requires improvement in many organisations. Organisations must take proactive measures to ensure that their employees are aware of the organisational direction and position regarding information security.

This theoretical foundation formed the baseline for the six proposed behavioural intention traits discussed. Theoretical propositions form the framework or the structure that can hold or support a theory from a research study. The theoretical proposition also helps to predict, explain and appreciate phenomena or to challenge and extend existing understanding within the limits of the critical underlying assumptions of the particular subject under study. A hypothesis is the research statement generated by researchers to try and speculate on the result of a research or an investigation. The research hypothesis can either be a null hypothesis (H0) or an alternative hypothesis (H1). For this article, six theoretical propositions were formulated from the six traits identified from the literature review as follows:

- **Proposition 1 (P1)**: Employee attitude towards information security is positively associated with the information security culture for the BYOD unintended administrator.
- **Proposition 2 (P2)**: Employee knowledge is positively associated with the information security culture in the BYOD phenomenon.
- **Proposition 3 (P3)**: The habits of the employee with regard to information security are positively associated with the information security culture in the BYOD phenomenon.
- **Proposition 4 (P4)**: The environment is positively associated with the information security culture in the BYOD phenomenon.
- **Proposition 5 (P5)**: Governance is positively associated with the information security culture in the BYOD phenomenon.
- **Proposition 6 (P6)**: The training offered to the employee by the organisation is positively associated with the information security culture in the BYOD phenomenon.

These propositions were tested using the statistical techniques of factor analysis, regression and correlation. The traits were then analysed. A discussion of the research methodology applied, follows next.

Research methodology

From the literature review conducted, the six components of attitude, knowledge, habit, environment, governance and training were identified and used to create six theoretical propositions, which were then used in the study. A questionnaire was designed from the literature review and used to conduct an electronic survey in a commercial bank in Zimbabwe. A population of 270 employees of the selected bank in Zimbabwe was chosen, making use of a convenience sampling method for the survey. A total of 205 employees participated in the study, and 179 of the responses obtained were deemed usable (i.e. a response rate of 87%). The data collected was subsequently loaded into SPSS version 23 for analysis, factor analysis and regression analysis. The Cronbach's alpha coefficient was used to measure reliability of the data. The next section discusses the statistical analysis conducted together with the findings of the research survey.

Statistical analysis

Demographic profile of the respondents

The results indicated that 60% of the respondents were male and 40% female. The majority of the participants fell into the age groups of 30–40 years, constituting 55% of the sample, and 41–50 years, constituting approximately 21% of the sample.

Most of the employees (89%) owned mobile devices while 92% of the employees confirmed that they understood the distinction between personal and organisational data and were able to keep them wholly separate while using a personal device for work.

The results were further subjected to reliability and validity tests.

Reliability and validity

Reliability addresses the dependability or repeatability of scores. Collis and Hussey (2013) view reliability as the consistency and accuracy with which a measure assesses a

particular variable. In research, validity addresses whether an instrument or test actually measures what it is intended to measure (Tsoukas 1989). According to Karlsson, Hedström and Goldkuhl (2016), validity refers to the accuracy of the measurement instrument, which is assessed by how it gauges a given variable and the extent to which it enables the researcher to make assumptions based on the findings. The Cronbach's alpha coefficient was used to measure the reliability of the factors. Table 2 shows the results of the reliability and validity.

The next section contains the results of the exploratory factor analysis (EFA) conducted on the traits.

A factor analysis of the traits

An EFA was used to identify and validate the traits for the model, as identified from the literature review. Prior to performing the principal components analysis, the suitability of the data for factor analysis was assessed. Inspection of the correlation matrix revealed the presence of many coefficients of 0.4 and above. The Kaiser–Meyer–Olkin measure was 0.754, which was above the recommended value of 0.6, and Bartlett's test of sphericity achieved statistical significance, confirming the factorability of the correlations matrix (Pallant 2011). Table 3 contains the results of the factor analysis.

The EFA was carried out to determine the validity of the traits and their related items. Principal components analysis showed the existence of six components that collectively accounted for 48.6% of the variance in the statistics. The principal components analysis conducted employed equamax with Kaiser normalisation as the rotation method. The rotated solution revealed six components with a number of items loading on each of the components, as portrayed in Table 3. The six factors were assessed and named according to the components.

TABLE 1: A demographic profile of the respondents.

Item	Category	Frequency	%
Gender	Male	106	59.0
	Female	72	40.0
	Did not answer	1	1.0
	Total	170	100.0
Age	< 30	29	16.2
	30–40	99	55.3
	41–50	37	20.7
	> 51	14	7.8
	Total	170	100.0
Employees who own a mobile device	Yes	159	88.8
	No	18	10.1
	Did not answer	2	1.1
	Total	170	100.0
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	100.0

TABLE 2: Reliability and validity.

Scale	Cronbach's rating	Number of items
Attitude	0.719	12
Knowledge	0.320	4
Habit	0.320	3
Environment	0.800	6
Governance	0.600	4
Training	0.720	6

Correlations between traits

Correlation coefficients give an indication of whether the relationship is positive (changes to traits increase or decrease in the same direction) or negative (traits respond in opposite directions). Pearson's correlation coefficient was thus used to investigate the relationship between the various factors. Table 4 contains the results of the correlation calculations conducted. The Pearson correlation coefficient (r) ranges from –1 to +1, with the sign in front of the numbers indicating whether there is a positive (as one variable

TABLE 3: Exploratory factor analysis results.

Items	Factors					
	Attitude	Environment	Training	Habit	Governance	Knowledge
ATT1	0.819	-	-	-	-	-
ATT2	0.818	-	-	-	-	-
ATT3	0.752	-	-	-	-	-
ATT4	0.723	-	-	-	-	-
ATT5	0.693	-	-	-	-	-
ATT6	0.612	-	-	-	-	-
ATT7	0.606	-	-	-	-	-
ATT8	0.514	-	-	-	-	-
ATT9	0.501	-	-	-	-	-
ATT10	0.466	-	-	-	-	-
ATT11	0.464	-	-	-	-	-
ATT12	0.410	-	-	-	-	-
ENV1	-	0.869	-	-	-	-
ENV2	-	0.796	-	-	-	-
ENV3	-	0.779	-	-	-	-
ENV4	-	0.613	-	-	-	-
ENV5	-	0.603	-	-	-	-
ENV6	-	0.460	-	-	-	-
TRAN1	-	-	0.851	-	-	-
TRAN2	-	-	0.801	-	-	-
TRAN3	-	-	0.644	-	-	-
TRAN4	-	-	0.520	-0.432	-	-
TRAN5	-	-	0.405	-	-	-
TRAN6	-	-	0.400	-	-	-
HAB1	-	-	-	0.679	-	-
HAB2	-	-	-	0.551	-	-
HAB3	-	-	-	-0.536	-	-
HAB4	-	-	-	0.535	-	-
HAB5	-	-	-	-0.405	-	-
GOV1	-	-	-	-	0.626	-
GOV2	-	-	-	-	0.601	-
GOV3	-	-	-	-	0.534	-
GOV4	-	-	-	-	0.411	-
KNOW1	-	-	-	-	-	0.560
KNOW2	-	-	-	-	-	0.509
KNOW3	-	-	-	-	-	0.505
KNOW4	-	-	-	-	-	0.402

ATT, attitude; ENV, environment; TRAN, training; HAB, habit; GOV, governance; KNOW, knowledge.

TABLE 4: Test of correlation between traits.

Variable	Description	Attitude	Environment	Training	Habit	Governance	Knowledge	Behavioural intention
Attitude	Pearson correlation	1	0.262**	0.270**	-0.059	0.327**	0.108	0.317**
	Sig. (two-tailed)	-	0.002	0.001	0.513	0.000	0.205	0.000
	N	145	138	137	126	132	140	141
Environment	Pearson correlation	0.262**	1	0.376**	0.045	0.350**	0.175*	0.356**
	Sig. (two-tailed)	0.002	-	0.000	0.608	0.000	0.031	0.000
	N	138	160	151	135	144	152	154
Training	Pearson correlation	0.270**	0.376**	1	0.246**	0.244**	0.189*	0.484**
	Sig. (two-tailed)	0.001	0.000	-	0.004	0.003	0.019	0.000
	N	137	151	161	139	146	153	154
Habit	Pearson correlation	-0.059	0.045	0.246**	1	0.185*	-0.138	0.071
	Sig. (two-tailed)	0.513	0.608	0.004	-	0.034	0.107	0.406
	N	126	135	139	145	132	138	139
Governance	Pearson correlation	0.327**	0.350**	0.244**	0.185*	1	0.041	0.342**
	Sig. (two-tailed)	0.000	0.000	0.003	0.034	-	0.618	0.000
	N	132	144	146	132	154	147	147
Knowledge	Pearson correlation	0.108	0.175*	0.189*	-0.138	0.041	1	0.085
	Sig. (two-tailed)	0.205	0.031	0.019	0.107	0.618	-	0.292
	N	140	152	153	138	147	163	156
Behavioural intention	Pearson correlation	0.317**	0.356**	0.484**	0.071	0.342**	0.085	1
	Sig. (two-tailed)	0.000	0.000	0.000	0.406	0.000	0.292	-
	N	141	154	154	139	147	156	165

*, Correlation is significant at the 0.05 level (two-tailed); **, Correlation is significant at the 0.01 level (two-tailed).

increases, so too does the other) or negative correlation. The size of the absolute value provides an indication of the strength of the positive or negative relationship (Pallant 2011). The Pearson correlation was used because the variables were suitably centred and normally distributed (Neuman 1997). The relationships were evaluated using Cohen's criteria (Salkind 2010):

- 0.1– small correlations
- 0.3 – moderate correlations
- 0.5 – large correlations
- 0.8 – extremely large correlations

A *p*-value *of* <0.05 was selected to indicate statistical significance. Based on this explanation, it can be concluded from Table 4 that the only significant and positive highly correlated relationship was evident between the dependent variables and the independent variable.

Behavioural intention is positively related to five of the six model traits, with the strongest positive relationship being with attitude (refer to Table 4). On the other hand, an inverse correlation between habit and behavioural intention was found. The next section discusses the regression analysis of the variables, which also helps understand which of the independent variables are related to the dependent variable.

Multiple regression analysis

Multiple regression describes how much of the variance in dependent variables can be explained by the independent variables. It also indicates the relative contribution of each independent variable. Tests were conducted to determine the statistical significance of the results in terms of both the model itself and the individual independent variables.

TABLE 5: Multiple regression analysis.

Independent variable	Beta	*t*	Significance (*p*)
Attitude	0.123	2.72	0.142
Habit	-0.59*	-0.721	0.472
Knowledge	-0.38*	-0.483	0.630
Training	0.381	4.353	0.00
Environment	0.127	1.476	0.143
Governance	0.176	2.06	0.041

t, Test statistic.

*, indicate that the results were identified as having an inverse relationship with the variables involved.

Table 5 presents a summary of the results of the multiple regression analysis and the variance analysis of the dependent variables. From the output presented in Table 5 it can be concluded that behavioural intention depends on the individual and organisational traits that collectively explain 32.1% ($R^2 = 0.321$) of the total output control.

Evaluation of theoretical propositions

The next phase of the statistical analysis involved the evaluation of the propositions formulated. The propositions each contribute to the subjective probability that information security will be treated as a culture when addressing BYOD security. Table 6 contains a summary of the theoretical proposition.

From the evaluation of the propositions, propositions P1, P4, P5 and P6 were found to be statistically positive and were accepted for inclusion in the BISB model, as all their statistical measurements showed positive results in explaining the relationships. Propositions P2 and P3 were rejected as they were not statistically explained. Although propositions P2 and P3 were rejected, owing to the results obtained from the literature review, they were deemed sufficient to explain the BISB model and were, therefore, retained as constructs of the model.

TABLE 6: Evaluation of research propositions.

Proposition	Cronbach's alpha	R^2	Beta	Result
P1 (attitude)	0.719	0.321	0.127	Accepted
P2 (habit)	0.390*	-0.590*	-0.059*	Rejected
P3 (knowledge)	0.320*	0.108	-0.460*	Rejected
P4 (training)	0.720	0.270	0.381	Accepted
P5 (environment)	0.800	0.262	0.127	Accepted
P6 (governance)	0.600	0.327	0.176	Accepted

*, indicate the results that were rejected.

Justification for retaining the attitude and habit traits

From the literature study conducted, sufficient support was provided by various authors to confirm the validity of attitude and habit in influencing behavioural intention. On attitude, Da Veiga and Martins (2014) maintain that an ISB consists of employees' attitudes and beliefs with respect to information security. Van Niekerk and Von Solms (2010) point out that attitude determines employees' ISB as it influences the level at which they observe the policy framework and the rules surrounding its implementation. In agreement with this perspective, Alfawaz et al. (2010) propose some ISB modes that organisations should observe.

On the habit trait, social theorists have agreed that people generally act habitually in the world, not reflectively (Hopf 2010). Findings from the study conducted by Keyes (2013) point out that human beings act habitually in their day-to-day functioning. Accordingly, BYOD has become part of the employee habits that drive the employees' day-to-day operations. In this regard, a survey conducted by Ovum (2014) has shown that BYOD has changed employee habits and expectations. The next section examines the refined BISB model, which constitutes the findings of this study.

The bring-your-own-device information security behavioural model

Figure 1 illustrates the combination of individual and organisational traits that culminate in a BISB model. In this model, the individual and organisational traits complement each other. The traits were identified from the literature study and then formulated into the behavioural intention traits that represent the BISB model. Attitude, environment, governance and training, as shown in the analysis contained in Tables 1 through 6, all displayed valid Cronbach's alpha, R^2 and beta values, whereas values related to attitude and knowledge were invalid. Nevertheless, these two traits were retained as valid model traits. These traits were then combined to formulate the BISB model shown in Figure 1. The BISB model is designed to present the components that are required for building a behavioural approach in managing the BYOD unintended administrator.

The BISB model is designed to present theoretically the components that are required for building an information security culture for the BYOD unintended administrator. The next section discusses the findings of this article.

Ethical consideration

Prior to conducting the survey, ethical approval was obtained from the bank, as well as the University of Fort Hare, South Africa.

Findings and discussion

The literature review identified the six independent variables of habit, knowledge, attitude, environment, governance and training, as well as one dependent variable, namely, behavioural intention. Various scholars share the belief that responsibility for information security has moved from the IT department to all employees (Dillon et al. 2015; Eslahi et al. 2015; Kritzinger & Von Solms 2012). Hence, many organisations are grappling with ways to secure the unintended administrator, who now carries information wherever he or she goes. From the statistical tests conducted, it was found that four of the six independent variables showed a positive correlation and valid regression patterns regarding the dependent variable. The *p*-values were also used to influence the decision to review and include the dependent variables in the model.

While technical solutions to the BYOD exist, an ISB approach cuts across all technical solutions as it addresses BYOD security at the source, which in this instance is at the unintended administrator level. From the tests conducted the six theoretical propositions were all deemed to be integral components of the BISB model. The statistical tests confirmed part of the traits as being valid model constructs, while the review of the various scholarly literature confirmed the other two traits of habit and knowledge.

Conclusion

The BYOD has turned the majority of employees into administrators of the devices they use. Although technical solutions exist, this article proposes an employee behavioural model in the form of the BISM model, which is a culmination of six independent variables and one dependent variable. The research was confined to one organisation and future work will include an evaluation of the model traits used. It will also explore the suitability of the traits selected to form the BISB model. The findings of this study could help to put in place proper governance structures in organisations to support employee involvement in the overall BISB model roll-out. Accordingly, organisations could choose an approach in which champions are appointed in the various departments to monitor and promote the BISB model roll-out. This could take the form of coordinated awareness campaigns and workshops. An employee who is aware, trained and involved, will automatically buy in and this will make handling the introduction of the BISB model easier. Depending on the

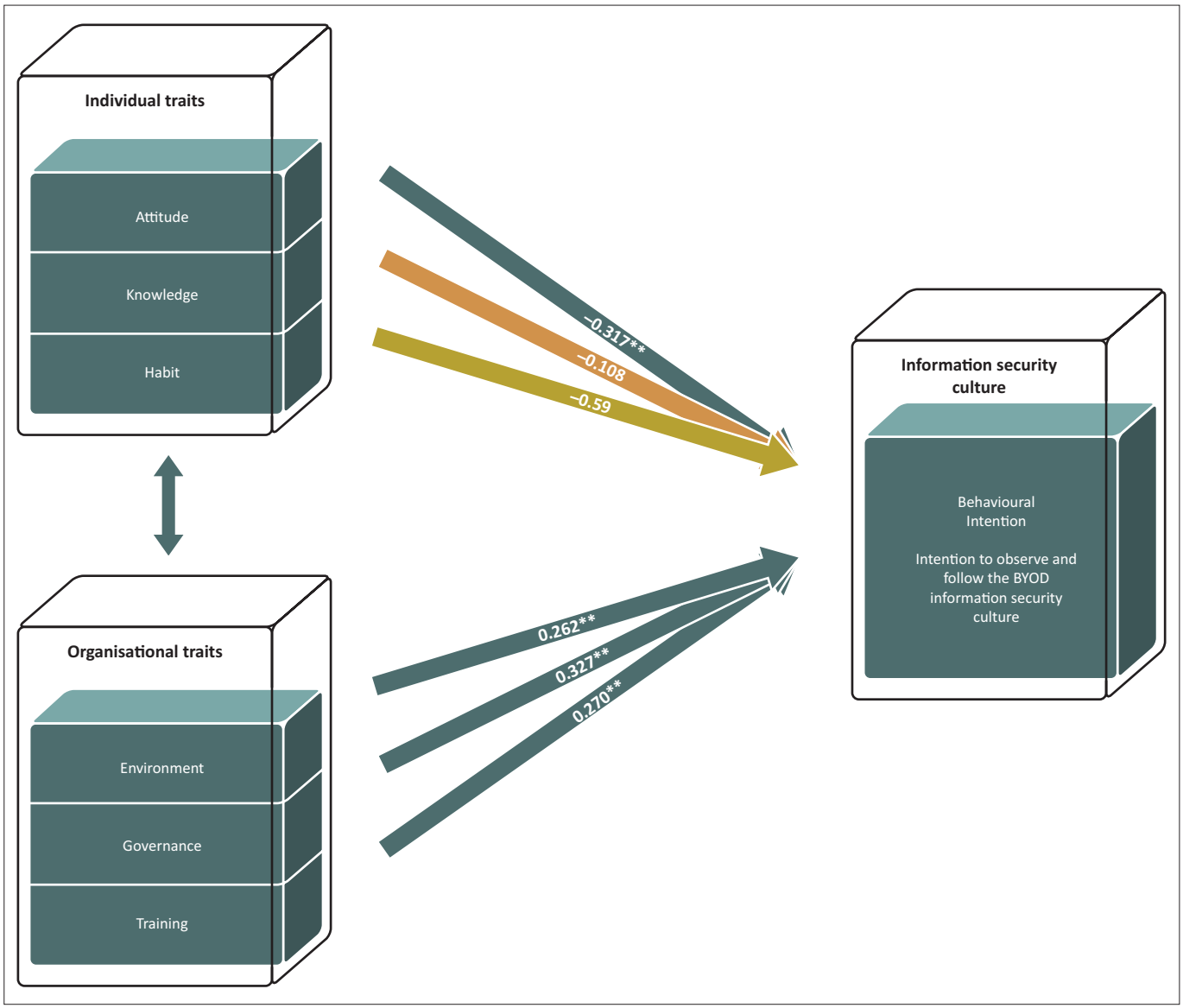

FIGURE 1: The 'bring-your-own-device' information security behavioural model.

organisation's structure, the training and development division of the human resources department in conjunction with the IT department could spearhead the roll-out of the BISB model in a classroom-like approach, which may then be followed by continuous assessment workshops. Several other approaches, not necessarily included in this document, could also be used to implement the BISB model in organisations. Future work will focus on testing the model applicability, as well as formulating means by which organisations can derive the best out of it. A maturity measurement mechanism will also be explored so that there will be a way for organisations to trace the performance and impact of the model.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contribution

S.F. provided conceptual input and supervised the study. A.M. contributed conceptual input, collected the data and wrote the article. L.C. contributed conceptual input and was the co-supervisor of A.M.

References

Ackerman, A. & Krupp, M., 2012, 'Five components to consider for BYOT/BYOD', in *IADIS International conference on cognition and exploratory learning in digital age (CELDA 2012)*, October 19–22, 2012, pp. 35–41, *International Association for Development of the Information Society*, New Jersey.

Agudelo, C.A., Bosua, R., Ahmad, A. & Maynard, S.B., 2015, 'Understanding knowledge leakage & BYOD (Bring Your Own Device): A mobile worker perspective', *The 26th Australasian Conference on Information Systems – ACIS2015*, Adelaide, November 30–December 04, 2015, pp. 1–13.

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

Alfawaz, S., Nelson, K. & Mohannak, K., 2010, 'Information security culture: A behaviour compliance conceptual framework', *Conferences in Research and Practice in Information Technology Series* 105(Aisc), 47–55.

Ajzen, I. & Fishbein, M., 1977, 'Attitude-behavior relations: A theoretical analysis and review of empirical research', *Psychological Bulletin* 84(5), 888.

Brodin, M., 2016, '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, December11–14, 2016.

Cheng, G., Guan, Y. & Chau, J., 2016, 'An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education', *Australasian Journal of Educational Technology* 32(4), 1–17. https://doi.org/10.14742/ajet.2792

Collis, J. & Hussey, R., 2013, *Business research a practical guide for undergraduate & postgraduate students,* 4th edn., Palgrave Macmillan, London.

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* 8(2014), 49–57.

Da Veiga, A. & Martins, N., 2015, 'Improving the information security culture through monitoring and implementation actions illustrated through a case study', *Computers and Security* 49, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

De Las Cuevas, P., Mora, A.M., Merelo, J.J., Castillo, P.A., García-Sánchez, P. & Fernández-Ares, A., 2015, 'Corporate security solutions for BYOD: A novel user-centric and self-adaptive system', *Computer Communications* 68, 83–95, https://doi.org/10.1016/j.comcom.2015.07.019

Dillon, S., Stahl, F. & Vossen, G., 2015, 'BYOD and governance of the personal cloud', *International Journal of Cloud Applications and Computing (IJCAC)* 5(2), 23–35. https://doi.org/10.4018/IJCAC.2015040102

Eslahi, M., Naseri, M.V., Hashim, H., Tahir, N.M. & Saad, E.H.M., 2015, 'BYOD: Current state and security challenges', in IEEE (ed.), *ISCAIE 2014 – 2014 IEEE symposium on computer applications and industrial electronics*, IEEE, Penang, Malaysia, April 07–08, 2014pp. 189–192.

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.

FinScope, 2014, *FinScope Consumer Survey Zimbabwe 2014*, Harare, viewed 01 February 2017, from https://finmark.org.za/finscope-zimbabwe-consumer-survey-2014/

Furst, L., 2013, *BYOD = 'Bring your own device'? or 'Bring your own disaster'?*, viewed 30 July 2016, from http://www.nstsystems.com/byod-bring-your-own-device-or-bring-your-own-disaster/

Garza, V. & Guo, X., 2015, 'Securing BYOD : A study of framing and neutralization effects on mobile device security policy compliance', *Icis-Rp* 1957, 1–10.

Gordon, J., 2015, *Top 3 mobility trends for 2016*, viewed 26 July 2016, from https://enterprisemobile.com/top-3-mobility-trends-for-2016/

Hopf, T., 2010, 'The logic of habit in international relations', *European Journal of International Relations* 16(4), 539–561. https://doi.org/10.1177/1354066110363502

Kaneshige, T., 2012, *BYOD: If you think you're saving money, think again*, viewed 01 February 2018, from https://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html#tk.drr_mlt.

Karlsson, F., Hedström, K. & Goldkuhl, G., 2016, 'Practice-based discourse analysis of information security policies', *Computers & Security* 67, 267–279.

Keyes, J., 2013, *Bring Your Own Devices (BYOD) survival guide*, vol. 6, Auerbach Publications, London.

Köffer, 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.

Kritzinger, E. & von Solms, B., 2012, 'A framework for cyber security in Africa', *Journal of Information Assurance & Cybersecurity* 2012(2012), 1–10.

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.

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, https://doi.org/10.1016/j.cose.2016.02.004

Lim, C.P. & Churchill, D., 2016, 'Mobile learning', *Interactive Learning Environments* 24(2), 273–276, https://doi.org/10.1080/10494820.2015.1113705

Musarurwa, A. & Jazri, H., 2015, 'A proposed framework to measure growth of critical information infrastructure protection in Africa', in *Proceedings of 2015 International conference on emerging trends in networks and computer communications, ETNCC 2015*, IEEE, Windhoek, Namibia, May 17–20, 2015, pp. 85–90.

Neuman, 1997, *Social research methods*, Oxford University Press, viewed 02 February 2017, from https://global.oup.com/academic/product/social-research-methods-9780199689453?cc=us&lang=en&

Ovum, 2014, *Beyond BYOD: How businesses might COPE with mobility – Identifying the right mobility strategy for your organization*, Informa, London.

Pahnila, S., Siponen, M. & Mahmood, A., 2007, 'Employees' behavior towards IS security policy compliance', in *Proceedings of the Annual Hawaii International Conference on System Sciences*, Honolulu, Hawaii, January 03–06, 2007, pp. 1–10.

Pallant, J., 2011, *SPSS survival manual. A step by step guide to data analysis using SPSS*, 4th edn., Allen and Unwin, Crowns Nest, Australia.

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 and Security* 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Salkind, N., 2010, *Encyclopedia of research design*, Sage, Los Angelos, CA.

Sophos, 2017, *A coming flood or a distant storm ? – The GDPR from a North American Perspective,* Sophos, Abingdon.

Tharp, B.M., 2009, 'Defining "culture" and "organizational culture": From anthropology to the office', *Interpretation a Journal of Bible and Theology* 1–5.

Tsoukas, H., 1989, 'The validity of idiographic research explanations', *The Academy of Management Review* 14(4), 551. https://doi.org/10.5465/amr.1989.4308386

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, https://doi.org/10.1016/j.im.2012.04.002

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

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

Von Solms, B. & Von Solms, R., 2004, 'The 10 deadly sins of information security management', *Computers and Security* 23(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Von Solms, R. & Van Niekerk, J., 2013, 'From information security to cyber security', *Computers and Security* 38(August), 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E. & Savangsuk, V., 2017, 'A policy-based framework for preserving confidentiality in BYOD environments: A review of information-security perspectives', *Security and Communication Networks* 1–11. https://doi.org/10.1155/2017/2057260

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