The BYOD Information Security Challenge for CIOs

A. Musarurwa and S. Flowerday

Department of Information Systems, Rhodes University, South Africa
e-mail: amusarurwa@hotmail.com; s.flowerday@ru.ac.za

Abstract

This paper highlights the way in which Chief Information Officers (CIOs) can mitigate the challenges that are posed by the Bring Your Own Device (BYOD) phenomenon. In terms of this phenomenon, employees inadvertently become unintended administrators as they have control of the devices they use. Previously, information security management was the preserve of the CIO and the Information Technology (IT) department, where trained IT employees managed all devices. Consequently, the advent of BYOD has shifted much of the responsibility from the IT personnel to the organisation's employees. This paper presents an employee behavioural management approach that CIOs may adopt to mitigate the BYOD information security challenges. This paper addresses the impact of BYOD, on the CIO's functional, transformational and strategic roles. Subsequently, an employee behavioural intention model is recommended as a way of mitigating these challenges. This BYOD Information Security Behavioural model, which was evaluated through an expert review process with CIOs in the Zimbabwe banking sector, encompasses six constructs: attitude, knowledge, habit, environment, governance and training.

Keywords

Bring Your Own Device (BYOD); General Data Protection Regulation (GDPR); Information Security Culture; Information Security Management

1 Introduction

Throughout the evolution of organisational information security management, the information technology (IT) administrator has always been the reference point for all IT issues and solutions (Jamf, 2017). The management of IT equipment and systems has been directed by an organisational policy framework owned by the Chief Information Officer (CIO). However, the advent of mobile devices has resulted in smartphones, phablets, tablets and many other mobile devices penetrating the organisational IT boundaries. As Ullman (2011) points out, the consumerisation of information technology has changed information security management in organisations, particularly as a result of the introduction of enterprise mobility through the bring your own device (BYOD) phenomenon. In this paper, BYOD is viewed as a phenomenon or new business practice by management which gives employees the privilege of using their own individual mobile devices to carry out work-related tasks (Alagbe, 2016).

In 2012, Gartner predicted that from 2018 the primary focus of endpoint breaches would shift to smartphones and tablets. In this evolution, Bongiorno, Rizzo, and Vaia (2018) highlighted that most organisations underestimate the risk faced in the BYOD

practice since they focus more on the devices being used than on the enterprise's entire mobility landscape, which includes their employees. A study conducted by PwC (2015) concluded that the BYOD practice has taught organisations numerous lessons across various industries, including retail, transportation, manufacturing, healthcare, and banking. Sathyan, Anoop, Narayan and Vallathai (2016) argue that enterprise mobility has been adopted by organisations to enhance their marketing channels, improve productivity in the office, boost customer satisfaction, as well as offer shopping experiences or process sales through the mobile devices. A customer survey on cybersecurity and enterprise mobility reported on by Zetlin (2017) found that half of the respondents used their personal devices for work, but they did not take basic security precautions, a fact made more worrying from a risk management perspective because 27% of those users reported having had their devices lost or stolen. All these exposures and challenges are posing serious information security challenges for CIOs.

This paper begins by introducing the BYOD unintended administrator and giving a purview of the challenges he/she poses. The paper then proceeds to explore the information security challenges faced by CIOs in a BYOD environment. The paper classifies the unintended administrator challenges into three key organisational roles for CIOs, namely, the functional role, the transformational role and the strategic role. The paper also briefly explores the impact of the General Data Protection Regulation (GDPR) on the CIO and BYOD information security. A recommendation on how to address these information security challenges is put forward in the form of an information security behavioural approach. The paper also discusses a survey conducted in the Zimbabwean banking sector and concludes with a recommendation for a BYOD information security behavioural (BISB) model which shows how CIOs can develop information security behaviour with regard to BYOD. The next section explores the BYOD unintended administrator in detail, presenting a case on how this has affected the CIOs.

2 The BYOD Unintended Administrator

Bongiorno et al. (2018) point out that the growth in mobile device usage has seen employees demanding to use their mobile devices on which to run critical business applications. The employees who own these devices carry critical applications used by the organisation and have thus become the unintended administrators of the organisation's information. The unintended administrator is not necessarily trained or aware of the information security risks and challenges that are associated with the BYOD phenomenon. This inadvertently shifts the management of the organisational information security from the information technology (IT) administrator to the unintended administrator. This shift leaves the organisation at risk of data and information security breaches which can permeate the organisation through the behaviour of these unintended administrators. Kaneshige (2016) contends that the uptake of BYOD is now pervasive and mission critical, leaving CIOs with the dilemma as to how to control the unintended administrator without simultaneously inconveniencing the business. Whilst the CIO and his team do not have direct control over the mobile devices being used in the BYOD practice, it remains the CIO's responsibility to make sure that the information contained in the devices as well as

their operation do not compromise the organisation's information security policies and standards.

3 Research methodology

The research approach followed in this paper was in the form of a literature review of the BYOD security challenges and an expert review where the experts were bank CIOs. The challenges that the CIOs face where identified and classified under the three CIO roles, namely, the functional, the transformational and the strategic roles. Accordingly, a questionnaire was created to identify the type of challenges that the CIOs face in these three roles. The questionnaire was then distributed to 18 CIOs in the Zimbabwean banking industry via Survey Monkey. From the 18 CIOs, a total of 18 complete responses were obtained. The results obtained are presented later in this paper.

4 CIO challenges in BYOD

Information security is the greatest challenge in the BYOD practice across all industries (Bauer & Bernroider, 2017). Costa, Merlo, Verderame, & Armando, (2015) point out that if the employees, who are viewed as unintended administrators in this paper, do not keep the device they use in the BYOD practice up to date with security software patches, that device becomes the most vulnerable point of the organisation's network. Studies conducted by Vorakulpipat, Sirapaisan, Rattanalerdnusorn, and Savangsuk (2017) have shown that most organisations are lagging behind in setting up comprehensive BYOD policies. They argue that the CIO's role is to ensure that the unintended administrator's productivity grows and the organisation remains competitive. Bongiorno et al. (2018) maintain that the CIO's role is increasingly becoming less functional, but more transformational and strategic. To achieve this portfolio shift, the CIO is faced with the task of harnessing the challenges that the unintended administrator brings and converting them into competitive benefits for the business. The CIO is also faced with the task of breaking down boundaries. A publication by the CIO.com (2018) states that "[t]he key to CIO success in modern-day business is to break boundaries. Boundaries between systems and data. Boundaries between business and IT. Boundaries between the status quo and new mandates for agility and transformation. Employees want their mobile devices to run the critical applications" (p. 2).

The following section considers the challenges that the CIO faces as a result of the influence of the unintended administrator. These challenges are classified under the three CIO roles. In the 2017 state of the CIO report, Muse (2017) shows that between 2010 and 2017 the CIO's roles moved from being 34% functional to being only 20% functional. At the transformational level, the CIO role was cited as having grown from 45% to about 50% and, on the strategic front, the role had grown from 21% to 31% in the same period. Table 1 below shows the year by year distribution of the CIO roles between the years 2010 and year 2017.

CIO roles	2010	2011	2012	2013	2014	2015	2016	2017
Functional (%)	34	43	23	19	19	22	27	20
Transformational (%)	45	46	23	56	47	52	45	50
Strategic (%)	21	11	25	25	34	27	27	31

Table 1: CIO roles between 2010 and 2017 (Muse, 2017)

Table 1 shows that there is a general shift in CIO roles from functional to more transformational and strategic roles. To delineate this impact, the next section explores these roles in more detail.

5 Impact of the GDPR on the CIOs role

The GDPR came into effect on the 25th of May 2018 replacing the existing data protection framework under the EU Data Protection Directive (Kingsley, 2018). This regulation emphasises transparency, security and accountability by data controllers at the same time strengthening the rights of the data owner over their data contained by organisations. The rights of the data owner under the GDPR include among other things, subject access, to have inaccuracies corrected, to have information erased, to object to direct marketing, to restrict the processing of their information, including automated decision-making as well as data portability (Data Protection Commissioner, 2018).

In this paper the CIOs main challenge is ensure the security of the data that is on the organisation's device. The rights that the user get through the GDPR put the CIO under a precarious position as some users may resists the CIOs control under the guise of the regulation. On a portable device, the organisational data co-exists with the user's data which therefore demands that the CIO must have a sophisticated means by which to meet both the organisational data security standards and the data owners' rights. The next section attends to the BYOD impact on the CIO's role profile.

6 Impact on the functional role of the CIO

The functional role of the CIO is basically the management of the business-as-usual tasks which form the day-to-day management of the IT functions. This includes establishing both stability and relevance for enterprise IT. Functional IT duties are not going away, but they are being minimised to some degree as a result of automation (HP, 2017). The functional roles include user support, security management and many other operations conducted daily. The BYOD practice has influenced the functional roles in the following areas:

i. Most employees involved in the BYOD phenomenon do not have permission from their organisation. Driven by their preferences, employees have begun

bringing their "shadow" devices of preference to the workplace, resulting in the rise of "Shadow IT". Trend Micro (2012) points out that, "[a]s consumerization proves to be irreversible, and threatens to become an IT nightmare by increasing security risk, data loss and financial exposure, it's clear that a lack of strategy could prove devastating. The best approach to effectively manage a consumerised workforce is to embrace consumerisation in order to unlock its benefits and reap its full business potential" (p. 1).

ii. Security and compliance costs are the direct responsibility of the CIO. In the BYOD practice, the CIO does not have total control of the mobile device, however the expectation remains that the organisation must be compliant with the information security and regulatory standards. Bagchi (2013) remarked that in the banking industry, compliance with regulation and the maintenance of a high standard of information security are primary requirements. If a bank embraces the BYOD policy, the CIO finds him/herself "caught between a rock and a hard place" as there is need for the organisation to leverage on the digital changes while at the same time retaining the integrity from a security perspective.

From a functional role perspective, the CIO is faced with some requirements that compromise the standard security rules. For example, there is a requirement to ensure that the operational standards are upheld while at the same time satisfying the business needs. The next section attends to the impact of the BYOD on the transformational role of the CIO.

7 Impact on the transformational role of the CIO

Today, CIOs are spending more time on transformational actions such as bringing in line IT initiatives with business goals and cultivating the IT and business partnership. Research on the 16th State of the CIO conducted by Muse (2017) found that CIOs are actively involved in driving customer acquisition and retention, leading and directing product innovation and collaborating on customer initiatives which transform the businesses. Managing the BYOD policy emerges as one such transformational role with which the CIO is tasked. In this transformational role, CIOs are faced with a range of challenges which are as a result of the existence of the unintended administrator. These include, but are not limited to, the following:

i. Embracing the cloud services for business agility. The unintended administrators make use of some cloud services which may be insecure for the organisation's documents. Examples of such include Dropbox, Google drive, One drive, iCloud and many others. In as much as these tools provide convenience and agility, they also expose organisational information to data loss and information theft (Bongiorno et al., 2018).

ii. Designing digital innovation is also one of the key roles that face the CIO. Bongiorno et al. (2018) contend that moving apps and workloads to the cloud, ensuring that legacy software can synchronise to off-premises apps, and keeping networks and systems secure remain the core functional tasks of the

CIO role. In this digital scramble, Muse (2017) also remarks that the boards of directors, chief executive officers and business colleagues are turning the CIO's role into a lead digital transformation driver to win customers and drive revenue growth.

In the transformational role, the CIO is faced with the challenge of ensuring that the business has the ability to offer the new services without compromising on the organisational policy standards. However, the unintended administrator accesses cloud computing services that may expose the organisation's security standards.

8 Impact of the strategic role of the CIO

CIOs are also focusing on strategic endeavours such as motivating business innovation and identifying strategic opportunities for competitive differentiation. Emerging technologies, such as artificial intelligence and the internet of things (IoT), generate headlines and the CIO is expected to drive the business strategic focus through them. The unintended administrator has compelled CIOs to drive strategic initiatives with a view to the security impact on the organisation at large. Stackpole (2017) purports that CIOs have, over the years, become the centre of digital innovation in organisations. This realisation entails an organisational requirement that the CIO remains competitive in the digital scramble, without putting the organisation at risk. Thus, the CIO needs to be vigilant and aware of the following strategic aspects:

i. CIOs are required to be the digital revolution drivers who improve the productivity of the employees without compromising the information for the organisation. The fact that the BYOD unintended administrator has disrupted the organisational strategic plans marks another "Achilles heel" for the CIO in trying to catch up. Wiech (2015) warns that the mobile devices have redefined the way banking is conducted, at the same time demanding a shift in information security management of the devices that interface with the banking systems.
ii. The unintended administrator at times acquires new mobile devices that are more sophisticated. In addition, they use devices from multiple vendors which makes it difficult for the CIO to keep track of the upgrades and maintenance. To drive the organisation's strategy, the CIO should be able to keep abreast of new innovations that satisfy the organisational strategic aspirations. Nevertheless, the unintended administrator is always ahead while the CIO follows.

The adoption of BYOD practice is blurring the line between work and personal life such that the information security boundary that is supposed to exist between work and personal life is now invisible. The challenges that are experienced by the CIO at the functional, transformational and strategic levels are all visibly influenced by the unintended administrator. To that effect, this paper recommends that the solution lies in addressing the administrator. In as much as the technical solutions exist for BYOD practice, Blizzard (2015) contends that technical solutions alone are not enough. There is need to attend to the unintended administrators' behavioural patterns in their usage

of the BYOD. The next section explores information security management and how CIOs can mitigate the challenges that emerge as a result of the existence of the unintended administrator.

9 A taxonomy for information security management in the BYOD

Singh and Phil's (2012) definition, which expresses information security as the standards for guarding data and information from illegal access, is used in this paper. Brien et al. (2013), believe that an "organisational culture that is information security aware will minimize risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets" (p. 2). Whilst allowing the BYOD practice holds many advantages and benefits for organisations, if not properly managed it will have disastrous consequences for organizations. In BYOD practice, the employee is the administrator and thus no endpoint security management policies can be enforced by the organisation's IT.

Olalere, Abdullah, Mahmod, and Abdullah (2015) argue that the biggest BYOD challenge is that organisational data are being delivered and managed by devices that are not managed by IT departments. They believe that these have security implications pertaining to data leakage, data theft and regulatory compliance, especially in the case of the banking industry. The GDPR sets out the responsibilities that organisations have in ensuring the privacy and protection of personal data, and also provides data subjects with certain rights, assigns powers to regulators to ask for demonstrations of accountability and even imposes fines in cases where organisations are not complying with GDPR requirements.

Inspired by inconsistencies in the current research on BYOD information security, Downer and Bhattacharya (2016) introduced a new taxonomy for classifying BYOD security challenges. This taxonomy divides BYOD information security challenges into two dimensions:

i. **Dimension 1:** Security challenges are categorised according to the areas of the organisation they affect most, such as the hardware or the software security as well as human resources.

ii. **Dimension 2:** In this dimension, challenges are classified by primary concern, key common characteristics and inferred relationships. For instance, equipment challenges are classified into deployment challenges and technical challenges. Deployment challenges are experienced prior to implementation while technical challenges are experienced during the entire BYOD lifecycle. The human resource challenge may be divided into policy and regulation challenges.

This paper expands on the human resource challenge, which has an impact on the organisational policies and regulations. In order to understand BYOD information security, all dimensions should be analysed in their respective stages. Several attempts

to address BYOD information security have concentrated on one of the two dimensions stated above. Figure 1 shows the proposed categories for BYOD security challenges.

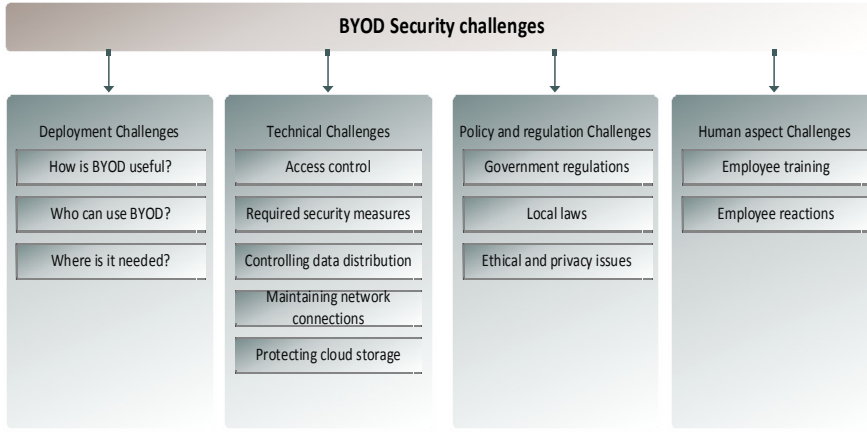

Figure 1. Taxonomies for BYOD Security Challenges (Downer & Bhattacharya, 2016)

Whilst the approach cited in Figure 1 addresses all the facets of BYOD practice, this paper proposes that there is a need to concentrate more on the challenges related to human aspects. Employee behaviour is something that needs attention as it determines how employees will implement all the other sections. This paper also proposes that measures to address human aspect challenges will not be sufficient unless they have been developed into a culture. Whilst training is important, a change in employee behaviour is crucial if BYOD security challenges are to be combatted. Provided behaviour is intentional, its occurrence may be predicted thus guiding the actions that ensue (Bada, Sasse, & Nurse, 2015). It may therefore be concluded that information security behaviour is probably the additional component of the model. Thus, information security regarding BYOD can be strengthened by exploring the two dimensions proposed by Downer and Bhattacharya (2016). In the technical dimension, existing security measures relating to BYOD practice are discussed in the following section.

10 How CIOs can mitigate the BYOD challenges

An organisation is driven by its culture and the unintended administrator forms part of this culture. Accordingly, in addressing BYOD challenges the first thing CIOs need to address is to make sure employees understand the organisation's regulations and policies. Secondly, this paper recommends that the organisational information security culture should be influenced in such a way that it supports a behavioural intention to heed the risks associated with BYOD. Thirdly, this paper recommends an operational component, namely, the implementation of a BISB model.

i. Understanding regulations: The European Union introduced the General Data Protection Regulation (GDPR)(EU) 2016/679, which is a regulation on data protection and privacy for all individuals within the European Union; it also addresses the exporting of personal data outside the EU (Overstraeten, Cumbley, & Pauly, 2016). Essentially, the EU GDPR is a set of rules on the way companies should process subjects' personal data.

ii. Understanding the organisational culture: Organisational culture (OC) is a widely documented topic the definitions of which are published in various contexts and industries. In the banking industry, OC is viewed as the shared beliefs and values that develop within the banking organisation. These beliefs and values guide the behaviour of its members in order to maintain suitable patterns in social systems to achieve coordinated behaviour aimed at survival in the dynamic environment. Another definition by Lundy and Cowling (1996) views OC as the way things are done in a particular organisation. This definition provides a casual but practical description of culture without necessarily providing an understanding of it.

iii. Building a BYOD information security culture: IT as a business enabler for organisations has become ubiquitous in today's workplace (Singh & Phil, 2012). The outcome of interactions between IT and OC can result in the acceptance and effective use of IT or user resistance, total rejection or even sabotage (Mehri & Yeganeh, 2015). Accordingly, when there is a misfit between IT and OC, three options exist:
   - reject the IT so as to seek one that is more compatible with the culture
   - redesign the technology before implementing it
   - proceed to adopt new IT options and face the challenges as they present themselves.

From the discussion it is clear that IT is a change agent for culture. The rate and direction of such change is basically driven by the rate of participation within the organisation. Another cardinal aspect of the impact of IT on culture is information security (Kuusisto & Ilvonen, 2003). It is therefore in the interests of every CIO to ensure that the organisation builds a culture with the behavioural intention to promote information security. The next section focuses on the constructs which were identified as central to building a BYOD information security culture.

11 Implementing a BYOD Information Security Behavioural (BISB) model

The operational way that the CIO can mitigate the challenges of the unintended administrator is through the implementation of a model that promotes the ultimate objective of securing the device. In developing this paper, a literature review was conducted on a commercial bank in Zimbabwe followed by a survey among CIOs in the banking industry in Zimbabwe as well. The results of the survey were subjected to statistical tests culminating in the identification of various individual and organisational traits. Ultimately, a set of six constructs was identified as follows:

1. **Attitude.** A study conducted by Allam, Flowerday and Flowerday (2014) suggests that attitude is dictated by what people think. In this paper, attitude refers to what employees think about BYOD information security; this includes the technology they use and the organisational policy framework.
2. **Knowledge.** Separate studies define knowledge as what people know (Allam et al., 2014; Kruger & Kearney, 2006; Safa, Von Solms, & Furnell, 2016). In this context, knowledge can be defined as what employees know about BYOD information security in a bank in Zimbabwe.
3. **Habit.** 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.
4. **Environment**. Organisational traits include the microenvironment, which was identified as being one of the key role players in the formulation of employee behavioural intention (Thomson, 2012). According to Farooq and Amin (2017), an appropriate environment is associated with a better information security culture.
5. **Governance.** Organisational governance is another key component identified as having an impact on information security behaviour. Information security management theorists assert that employee behaviour needs to be 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).
6. **Training.** Training on the information security plan for the organisation is another key component identified in the literature review as a pillar on which an information security culture is built. Because employees come from different backgrounds, many of them lack basic awareness of the consequences of breaching information security guidelines (Al-shehri, 2012).

12 Behavioural intention

Many studies focus directly on the individual as the locus of behaviour. According to Tharp (2009), that complex whole which includes knowledge, belief, arts, morals, law, custom, and any other capabilities and habits acquired by man as a member of society forms the behavioural intention which can be summed up as a culture. The literature review conducted for this paper uncovered links between culture and information security behavioural intention. This behavioural intention thus translates into the security culture exhibited by employees in the organisation.

Figure 2 illustrates the combination of individual and organisational traits culminating in a BYOD information security behavioural (BISB) model. These constructs were explored individually and found to contribute to the behavioural intention of employees.

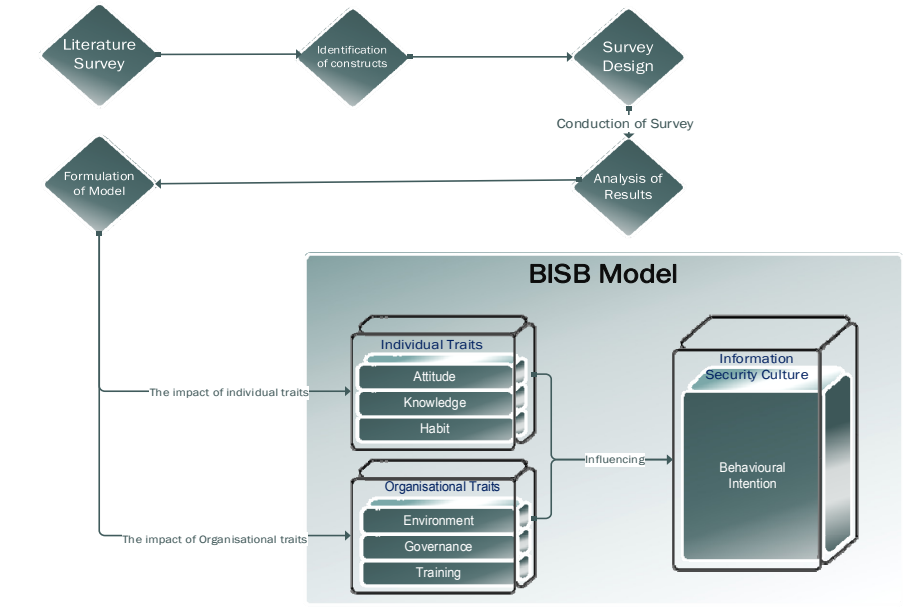

Figure 2: The BYOD Information Security Behavioural Model (BISB)

As Figure 2 shows the research process followed culminating into, individual and organisational traits which were combined to form the BISB model. The next section gives a high-level analysis of the findings from the survey conducted on CIOs in the Zimbabwe banking sector.

In this survey, a set of questions were distributed to 18 CIOs. The questions were designed to obtain an understanding of the spectrum of challenges that CIOs face in their functional, transformational and strategic roles. The next section presents the qualitative analysis of the findings.

13 Analysis and Findings

From the findings presented above it is clear that the CIO is definitely in need of a model or framework that ensures that the information security and data security standards for their organisations are not compromised. The promulgation of the GDPR shifted the pendulum of data control towards the data owner. To this end, implementing and enforcing information security standards that support adherence to a high information security mitigation becomes difficult for the CIO. This paper premised the BYOD challenges on three CIOs roles profiles which are the functional role, the strategic role as well as the transformational role. The findings of the survey revealed all three role components. From a functional role perspective, BYOD has shifted from the management of devices distributed by the IT department to a position where every employee who owns a device participates in the BYOD. Accordingly, IT functions have become more complex and dependent on the goodwill of the

unintended administrator. From a transformational perspective, BYOD has acted as a vehicle for transformation, as it enables the CIO to roll out the products and services that the organisation consumes. For instance, in a bank where customer relationship managers want to open bank accounts on the move, they can make use of a mobile device to capture and scan documents instantly. From a strategic perspective, BYOD has become an enabler of strategy implementation. Ultimately, the biggest challenge remains information security. The paper proposes an Information security behavioural model along six traits of attitude, knowledge habit, environment governance and training. These traits were deemed to be instrumental in influencing the employee's behavioural intention towards the BYOD information security.

Table 2 shows results of a survey conducted in the Zimbabwe financial services sector along a five-point likert scale showed that about 70% of the CIOs agreed that the BISB model can be applied to mitigate the information security challenges faced by the CIOs on the BYOD.

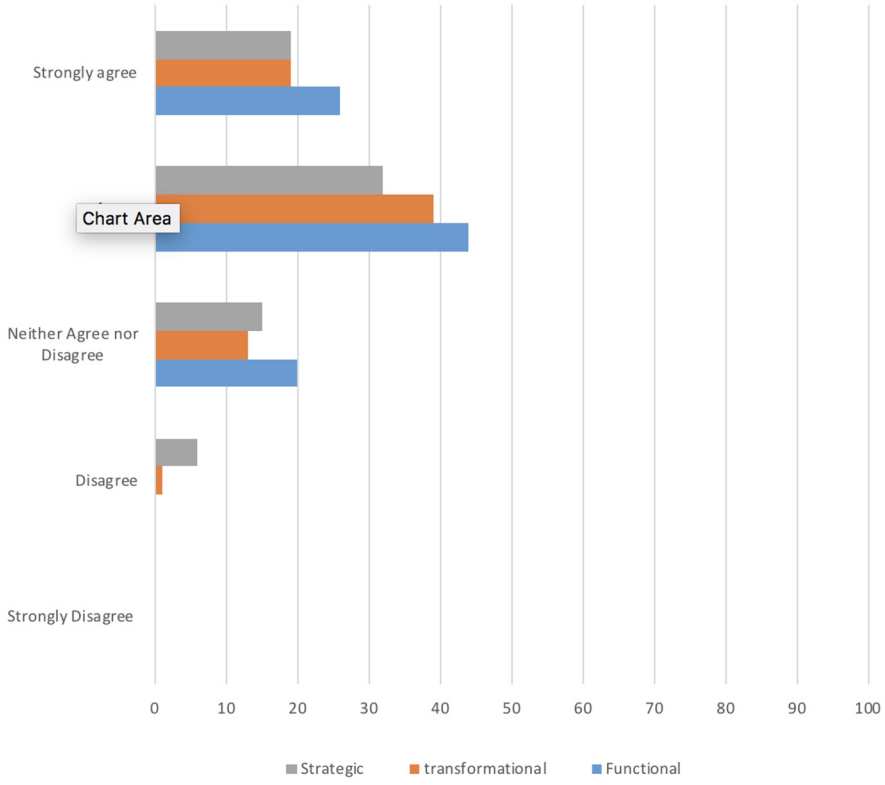

Figure 3: Analysis and Findings

Figure 3 shows a high-level presentation of the survey results. As the figure shows, the CIOs generally agreed that BYOD does affect their functional, transformational and strategic roles. The majority of CIOs felt that most of the challenges experienced

were in relation to the CIO's functional role. Table 1 below shows the responses per question regarding each role profile.

Functional	**Completely Disagree**	**Disagree**	**Neither Agree Nor Disagree**	**Agree**	**Completely Agree**
With regulations like the GDPR and PCDISS, which aim for complete protection of consumer data and adherence to strict standards. In a BYOD enviromnent,these standards can be upheld.	0	0	4	11	3
Bring Your Own Device (BYOD) is a rapidly growing trend with benefits to the organisation but it introduces risk to the organisation. The risks out weigh the benefits.	0	0	5	12	1
BYOD unneccessarily increases the organization's management effort, both for maintaining an accurate inventory of the devices, keeping operating systems' software up-to-date and supporting the increasing number of device types.	0	0	7	6	5
In BYOD users should not be allowed to install their own personal applications on their devices but they should install only whitelisted applications by the organisation	0	0	4	4	10
The notion of the 'unintended administrator' inherent in BYOD poses a challenge to the success of BYOD. CIOs should put policies in place to ensure the user devices are compliant to the organisational policies. Do you agree?	0	0	0	11	7
Transformational	**Completely Disagree**	**Disagree**	**Neither Agree Nor Disagree**	**Agree**	**Completely Agree**
Making the necessary organizational changes to adopt BYOD may require a shift away from centralized systems towards more open enterprise systems and this change can present challenges to enterprises in particular over security, control, technology and policy to the traditional IT model within organisations. Do you agree?	0	1	3	8	6
Organistional culture can be a barrier to implementing BYOD policies. To successfully implement BYOD, CIOs must have buy in from employees and other stakeholders to successfully transform their organisations. Do you agree?	0	0	1	10	7
There is a risk that BYOD policies can infringe on the privacy of employees in the name on corporate data protection, what strategies can CIOs implement in order to curb against infringing on user's private information	0	0	5	11	2
BYOD represents a fairly new way of doing things in organisations.Management of its implemenation is of paramount importance if it is to be a success	0	0	4	10	4
Strategic	**Completely Disagree**	**Disagree**	**Neither Agree Nor Disagree**	**Agree**	**Completely Agree**
The strategic importance of BYOD cannot be ignored but the threats it poses to enterprise security cannot be ignored as well. The strategic importance of BYOD outweighs the associated risks	0	0	2	10	6
BYOD requires CIOs to make modifications to the current IT infrastructure so that it's BYOD compliant. CIOs do not need to identify which applications their employees are using to interact with corporate data.	0	0	4	7	7
In BYOD, understanding the sensitivity of your data and setting appropriate security measures will help to ensure that your intellectual property is not compromised. For example, in a Banking environment, customer information is of paramount importance. In this vein, BYOD cannot be successifully implemented in all environments including banks?	**0**	**6**	**3**	**9**	**0**
BYOD is seen as a benefit for employees that increases employee loyalty. Do you agree?	0	0	6	6	6

Table 2: CIO Survey Responses

Table 2 show the questions which were used to conduct the survey. The results were then presented in Figure 2. From the spread of the results the analysis positively confirms that the CIO's role will be made easier if there is an operational model around the BYOD.

The findings from the literature review conducted as well as the analysis of the CIO role suggest that the CIO indeed require a people driven approach towards mitigating the BYOD information security challenges as across the CIOs role profile cited in this paper as follows:

- Functional role: On a functional role perspective, the CIO requires the right attitude from the devices users in order for him to be able to mitigate the BYOD information security risks. Knowledge is also needed to create the requisite environment to create the correct habits among the employees from an organisational governance framework that allows training.
- Strategic role: The strategic role also requires the rightful attitude from the employees coupled with the appropriate habits that promote information security. These will be in an environment that offers the correct training on knowledge around the information security risks and information security governance.
- Transformational role: For every organisation to transform, there is need for the correct habits towards information security, which are also coupled with the knowledge, governance and the training to satisfy the organisation's strategic aspirations

From the summary above the findings indeed point to the fact that building an information security aware behavioural intention is an important solution that the CIO can embrace. This paper therefore proposes that CIOs should adopt the BISB model.

14 Conclusion and Future Work

This paper focused on the impact of the BYOD on the three CIO roles. It may accordingly be noted that if effective security behaviour is practised over time, an information security culture may result, as advocated by the BISB. As this model recommends, when an organisation builds an information security culture for the unintended administrator, the three individual traits and three organisational traits should be considered. Whilst the CIO's role is evolving gradually towards transforming the organisation through strategic digital offerings, the unintended administrator remains the primary challenge in their fulfilment of the new role. This paper also noted that there are technical solutions that can be used in BYOD practice but recommends that the real solutions in addressing the unintended administrator is through the BISB model.Future work will include additional tests on the CIO roles. Attention will also be given to the regulatory and policy impact of the BYOD. Furthermore, since the introduction of the GDPR by the European Union on 25 May 2018 marked a new era in data protection laws globally, the impact of the GDPR on BYOD and the CIO roles will be a point of focus.

15 References

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

Alagbe, A. (2016). The Security Implication of BYOD : Mobile Devices in the Workplace. University of Strathclyde, Glasgow.

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

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? Proceedings of the International Conference on Cyber Security for Sustainable Society. London.

Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action : Analyzing Information Security Policy Compliance in a Large Banking Organization, (October 2016). http://doi.org/10.1145/3130515.3130519

Beth Stackpole. (2017). CIOs adjust to their new reality | CIO. Retrieved February 3, 2018, from https://www.cio.com/article/3162718/cio-role/state-of-the-cio-2017-the-new-reality.html

Blizzard, S. (2015). Coming full circle: Are there benefits to BYOD? Computer Fraud and Security, 2015(2), 18–20. http://doi.org/10.1016/S1361-3723(15)30010-5

Bongiorno, G., Rizzo, D., & Vaia, G. (2018). CIOs and the Digital Transformation: A new Leadership role (1st ed.). Milan, Italy: Springer International Publishing.

Brien, J. O., Islam, S., Bao, S., Weng, F., Xiong, W., & Ma, A. (2013). Information security culture: Literature Review. Minerva. Melbourne.

CIO.com. (2018). The modern CIO's role is more challenging than ever. Retrieved February 3, 2018, from https://hybridit.cio.com/transformation

Costa, G., Merlo, A., Verderame, L., & Armando, A. (2015). Automatic security verification of mobile app configurations. Future Generation Computer Systems. http://doi.org/10.1016/j.future.2016.06.014

Crawshaw, J., Budhwar, P., & Davis, A. (2017). Human Resource Management : Strategic and International Perspectives. (Jonathan Crawshaw, P. S. Budhwar, & A. Davies, Eds.)Sage Publications Ltd. London, United Kingdom: Sage Publications Ltd.

Data Protection Commissioner. (2018). The GDPR and You, 11. Retrieved from https://www.dataprotection.ie/docs/30-11-2016-GDPR-and-You-Preparing-for-2018/1604.htm

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.

Downer, K., & Bhattacharya, M. (2016). BYOD security: A new business challenge. In 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communic (pp. 1128–1133). New York, USA: IEEE.

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.

Gartner. (2012). Enterprise Mobility : Trends, Challenges and Solutions Gartner at a Glance. Las Vegas.

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

HP. (2017). The Strategic CIO' s Playbook Table of Contents.

Jamf. (2017). Conditional Access : Going Beyond Perimeter-Based Security The Modern Workplace and the Next Generation of Security.

Kingsley. (2018). An introduction to the General Data Protection Regulation.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25(4), 289–296. http://doi.org/10.1016/j.cose.2006.02.008

Kuusisto, T., & Ilvonen, I. (2003). Information Security Culture in Small and Medium Size Enterprises. Frontiers of E-Business Research, 431–439.

Mehri, B., & Yeganeh, E. (2015). The impact of national and organizational culture on information technology (I) Abstract : Karaj.

Minda Zetlin. (2017). State of the CIO 2017: Priorities that can't wait | The Enterprisers Project. Retrieved February 3, 2018, from https://enterprisersproject.com/article/2017/4/state-cio-2017-priorities-cant-wait

Muse, D. (2017). State of the CIO: 2017. Idg, 1–12. Retrieved from http://core0.staticworld.net/assets/2017/02/20/state_of_the_cio_exec-summary_2017.pdf

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. SAGE Open, 5(2), 11.

Overstraeten, T. Van, Cumbley, R., & Pauly, D. (2016). The General Data Protection Regulation: A Survival Guide.

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 (pp. 1–10). Honolulu, Hawaii.

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

Rastogi, R., & Von Solms, R. (2012). Information Security Service Culture – Information Security for End-users. Journal of Universal Computer Science, 18(12), 1628–1642.

Sathyan, J., Anoop, Narayan, N., & Vallathai, S. K. (2016). A Comprehensive Guide to Enterprise Mobility. (CRC Press, Ed.)Infosys press (An Auerbac). Boca Raton: CRC Press.

Singh, M. N., & 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.

Sohini Bagchi. (2013). Public Banks still skeptical of BYOD. Retrieved January 18, 2018, from http://www.cxotoday.com/story/banking-sector-in-india-still-wary-of-byod/

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56, 1–13. http://doi.org/10.1016/j.cose.2015.10.006

Symantec. (2012). 2012 Norton Cybercrime Report. Norton Cybercrime Report. Massachusetts.

Tharp, B. M. (2009). Defining " Culture " and "Organizational Culture": From Anthropology to the Office. Interpretation a Journal of Bible and Theology, 1–5.

Thomson, G. (2012). BYOD: Enabling the chaos. Network Security, 2012(2), 5–8. http://doi.org/10.1016/S1353-4858(12)70013-2

Tom Kaneshige. (2016). CIO Challenge with BYOD: Don't Fall Down the Rabbit Hole | CIO. Retrieved February 1, 2018, from https://www.cio.com/article/2395938/byod/cio-challenge-with-byod--don-t-fall-down-the-rabbit-hole.html

Trend Micro. (2012). Consumerization Survey Report The Consumerization of IT, 1–8.

Ullman, E. (2011). BYOD and Security. Tech & Learning (Vol. 31).

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. http://doi.org/10.1016/j.im.2012.04.002

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, 2017. http://doi.org/10.1155/2017/2057260

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

Wiech, D. (2015). Banks and others accounting for BYOD. Retrieved July 30, 2016, from http://www.it-director.com/content/banks-and-others-accounting-for-byod/