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

Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries

Authors:
Willard Munyoka[1]
Manoj S. Maharaj[2]

Affiliations:
[1]Department of Business Information Systems, University of Venda, Thohoyandou, South Africa

[2]School of Management, IT and Governance, University of KwaZulu-Natal, Durban, South Africa

Corresponding author:
Willard Munyoka,
wmunyoka@gmail.com

Dates:
Received: 19 Mar. 2018
Accepted: 10 Oct. 2018
Published: 14 Mar. 2019

How to cite this article:
Munyoka, W. & Maharaj, M.S., 2019, 'Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries', *South African Journal of Information Management* 21(1), a983. https://doi.org/10.4102/sajim.v21i1.983

Background: Many Southern African Development Community (SADC) countries are adopting and implementing e-government systems to improve the efficiency and effectiveness of their service delivery systems, and Zimbabwe and Zambia are not an exception. However, scholars have noted that the acceptance and utilisation of e-government systems by citizens in Zimbabwe and Zambia is affected by many factors, among others, perceived privacy, perceived security, perceived trust, perceived risk and optimism bias.

Objectives: The aim of this study was to investigate the effect of privacy, security, trust, optimism bias and perceived risk on citizens' use behaviour of e-government systems in the SADC.

Method: This study proposes an e-government utilisation model. A quantitative design was employed to collect data from a survey of 489 e-government users in Zambia and Zimbabwe to test the model fit using structural equation modelling.

Results: Perceived lack of privacy, security, trust; perceived risk and optimism bias were all confirmed as salient factors affecting the utilisation of e-government systems by citizens in Zambia and Zimbabwe. The structural equation model results confirmed the model fit of the proposed e-government research model. All eight hypotheses for this study were confirmed.

Conclusion: The findings of this study provide pointers to practitioners, decision-makers and policymakers on e-government matters on the need to seriously consider privacy, security, risk and trust issues of e-government systems to encourage the utilisation of such systems by citizens.

Introduction

Electronic government (e-government) can provide quality services to citizens when and where needed. E-government is recognised as a fundamental tool to encourage citizen participation in public service delivery matters (United Nations 2016b) and millions of dollars are being invested annually in e-government projects across the world (World Bank 2016). However, e-government adoption by citizens (G2C) remains very low (Shalhoub 2006; World Bank 2016). The established primary reasons for this are security concerns, trust issues, risk factors and privacy issues (Shalhoub 2006; Zafiropoulos, Karavalisis & Vrana 2012). However, there are other factors (Bwalya 2017; Munyoka & Maharaj 2017) affecting the use of e-government by citizens.

This study investigated how privacy, security, trust, risk and optimism bias factors are affecting citizens' perceptions and decisions to use e-government systems in Zimbabwe and Zambia. The keyword 'perceived' prefixed on each construct (e.g. perceived security) refers to both citizens' perceptions and actual experience. The results of this study would be significant to practitioners, decision-makers and policymakers who seek to strengthen the G2C relationships in developing countries.

This article is structured as follows: firstly, the theoretical underpinnings are laid out for the study. Then the research model and hypotheses followed by the research methodology are presented. The findings of the empirical study are then presented and discussed.

Theoretical underpinnings

The complex nature of the G2C phenomenon requires multiple models to help interpret the data collected. This study draws from several models: the National Initiative for Cybersecurity Education cybersecurity capability maturity models (NICE-CMM) and National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST 2018; US Department of

Homeland Security 2014), the extended unified theory of acceptance and use of technology (UTAUT2) (Venkatesh, Thong & Xu 2012) and the affective decision-making theory of optimism bias and risk (Bracha & Brown 2012). A summary of these models and their relevance to this study is now presented.

National Initiative for Cybersecurity Education and Cybersecurity Capability Maturity Model

The US Department of Homeland Security's NICE-CMM model is a toolkit that is widely used at both national and organisational (both public and private) levels in the EU, USA, UK and Canada for establishing cybersecurity policies, strategic planning and providing guidelines for training all stakeholders. The NICE-CMM model is applied mainly at the organisational level to build citizens' trust in G2C.

The National Institute of Standards and Technology Cybersecurity Framework

This framework provides a set of core activities aimed at developing individual cybersecurity skills (National Institute of Standards and Technology 2018:2). This framework provides key construct items for the perceived security construct of the study.

The affective decision-making theory of optimism bias and risk

Affective decision-making (ADM) is a strategic model predicting an individual's rationale for undertaking certain utility choices under risk (Bracha & Brown 2012). The ADM theory asserts that the interaction between the rational and emotional cognitive processes determines an individual's choice regarding the utilisation of a specific service. Optimism bias is the belief that prior experience in using a specific system makes the user less vulnerable to risks compared to an average user (Carlin 2016). Hence, when individuals are confronted with risky choices the rational approach determines one's action and the emotional process informs one's perceptions of risk; combined together, this makes an individual optimistically biased. The ADM theory is pertinent in understanding and defining the perceived risk and optimism bias construct variables for the research model in Figure 1.

The extended unified theory of acceptance and use of technology model

The UTAUT2 model consists of seven constructs (performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value and habit) and three moderating variables (age, gender and education)

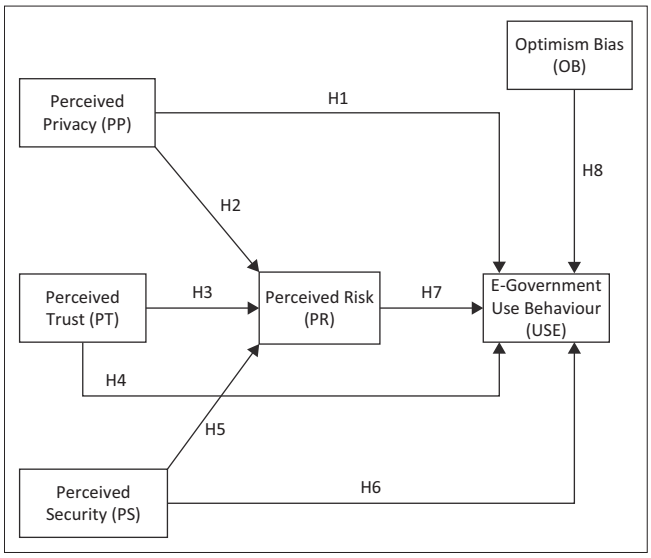

FIGURE 1: E-government use research model.

that influence an individual's decisions for adopting and using a system. The UTAUT2 illustrates how these factors play a pivotal role in informing users' decisions towards adopting any e-system. The UTAUT2 model is adapted to suit the context of this study, in line with cybersecurity considerations in adopting and using e-government systems.

In the context of this study 'use behaviour' (Shareef et al. 2011) refers to a citizen's disposition in accepting and continually using e-government systems as the primary means for accessing government services. This study is guided by the following research questions:

- What effect does perceived privacy have on e-government use behaviour?
- What effect does perceived trust have on e-government use behaviour?
- What effect does perceived security have on e-government use behaviour?
- What effect does perceived risk have on e-government use behaviour?
- What effect does optimism bias have on e-government use behaviour?
- What effect does perceived privacy, security and trust have on perceived risk?

To answer these research questions, several null hypotheses were established for each construct as outlined in the next section.

Research model and hypotheses

Privacy

Papadomichelaki and Mentzas (2012:100) define 'privacy' as the 'protection of personal information, not sharing personal information with others, protecting anonymity, secure archiving of personal data, and providing informed consent'. Prior research indicates that the public required assurance of adequate privacy protection embedded in e-government systems prior to and when using them (ITU 2012; Majdalawi

et al. 2015; Ramli 2017). Moreover, any perception of inadequate privacy tends to increase the perceived risk of using e-government systems, leading to eroded trust and a lack of desire to use such systems (Ewurah 2017). To overcome such privacy worries, the incorporation of a privacy statement on e-government websites addressing all fundamental privacy principles, compensation mechanisms, government regulations and ICT self-regulation for enforcing procedural justice for perpetrators is recommended (Bansal, Zahedi & Gefen 2010; Shalhoub 2006; Xu et al. 2009). Therefore, to promote e-government acceptance and utilisation by citizens, governments in the Southern African Development Community (SADC) region should ensure the privacy of personal information, data and transactions. Therefore, in line with privacy, two hypotheses are proposed:

$H1_0$: Perceived privacy has no influence on use behaviour on e-government systems.
$H1_a$: Perceived privacy influences use behaviour on e-government systems.
$H2_0$: Perceived privacy has no influence on perceived risk of e-government systems.
$H2_a$: Perceived privacy influences perceived risk of e-government systems.

Trust

Trust focuses on the confidence that citizens have in e-government systems concerning freedom from any risk of danger, doubt or fraud during a transaction (Papadomichelaki & Mentzas 2012). Al-Zoubi (2008) suggests that trust is one of the most important catalysts affecting citizens' decisions to adopt and use e-government systems. The importance of trust as a decisive factor in determining the success or failure of e-government has been reiterated in other studies (Fakhoury & Baker 2016; Shalhoub 2006; Zhao & Zhao 2010). The measure of trust is based on two fundamental aspects: the trust in the Internet and the trust in the e-government system. As in most prior studies on e-commerce and e-government adoption and use, perceived trust is expected to have a positive effect on both behavioural intention to adopt and use behaviour (Al Khattab et al. 2015; Anthopoulos et al. 2016; Colesca 2009) and to reduce perceived risk (Schaupp & Carter 2010).

$H3_0$: Perceived trust has no influence on perceived risk of e-government systems.
$H3_a$: Perceived trust influences perceived risk of e-government systems.
$H4_0$: Perceived trust has no influence on use behaviour of e-government systems.
$H4_a$: Perceived trust influences use behaviour of e-government systems.

Security

Security is concerned with administrative and technical procedures, associated with protecting data and information against possible losses, 'unauthorised access, destruction, use, or disclosure' (Shalhoub 2006:272). In the context of e-government, administrative issues are concerned with formulating, implementing and reviewing information and data security policies. These policies are the cornerstone of effective cybersecurity measures needed for building citizens' trust in e-government (Singh & Karaulia 2011). Technical procedures are essential for e-government systems to prevent unauthorised access to databases and transactions, and these include preventing unauthorised access through the use of encryption, limiting access to passwords and securing servers and the network infrastructure. In developing countries where high levels of corruption are reported (Mistry & Jalal 2012; Pathak et al. 2008), stringent administrative and technical procedures are essential for building citizens' trust in e-government. Similarly, citizens are bound to use e-government systems that they perceive to be secure (Schaupp & Carter 2010). In line with this discussion on security, two hypotheses are proposed:

$H5_0$: Perceived security has no influence on perceived risk of e-government systems.
$H5_a$: Perceived security influences perceived risk of e-government systems.
$H6_0$: Perceived security has no influence on use behaviour of e-government systems.
$H6_a$: Perceived security influences use behaviour of e-government systems.

Perceived risk

ICT risks are related to the possibility that a system is inadequately protected from different types of threats (Schaupp & Carter 2010). Similarly, perceived risk is the belief that one will experience some losses whilst interacting with an e-system and that is caused by one's perceptions of the privacy and security of such a system. Almarashdeh and Alsmadi (2017) further assert that once citizens perceive high risk in using an e-government system, there is a general tendency of postponing the transaction and resorting to an alternative medium. Considering the uncertainty that besieges online-based transactions and the vast potential of cyberattacks, this study suggests that perceived risk has a significant impact on one's decisions to adopt and use e-government systems. Several studies (Al Khattab et al. 2015; Schaupp & Carter 2010) established that risk perception has a negative effect on one's use behaviour of e-government systems.

$H7_0$: Perceived risk does not have an effect on citizens' use behaviour of e-government systems.
$H7_a$: Perceived risk has an effect on citizens' use behaviour of e-government systems.

Optimism bias

Optimism bias defines 'a systematic error in perception of an individual's own standing relative to group averages, in which negative events are seen as less likely to occur to the individual than average compared with the group, and positive events as more likely to occur than average compared with the group' (Weinstein 1980:809). Prior studies demonstrate that despite high perceptions of risk and reported cases of cyberattacks (Alsaghier et al. 2009; Carlin 2016; Hassan & Khalifa 2016), people with experience of

using online services do not believe that they are susceptible to attacks compared to the average user. Therefore, in terms of e-government adoption and utilisation, citizens who regard themselves to be more Internet savvy, compared to the average user, will be less deterred by perceived risks and thus tend to use such systems. Practically, optimism bias is measured by asking participants to compare their capabilities in executing an online task with that of an average user.

$H8_0$: Optimism bias does not have an effect on citizens' use behaviour of e-government systems.

$H8_a$: Optimism bias has an effect on citizens' use behaviour of e-government systems.

Research model

Considering the aforementioned corpus of literature and insights from the theoretical underpinnings, this article posits that citizens' use behaviour of e-government systems is affected by their perceptions and lived experiences of the privacy, security and trust in such systems. However, because of the effect of optimism bias, citizens are inclined to pursue the use of e-government systems. Hence, Figure 1 presents the proposed research model for this study.

Research methodology

A quantitative research design (Creswell 2014) and deductive approach (Gelo, Braakmann & Benetka 2008) underpin this study. Data was collected from 550 citizens from the two SADC member states using self-administered semistructured questionnaires. Multistage sampling techniques were used to identify the 550 participants. The questionnaire was comprised of two sections: Section A covered demographic-related questions, and Section B consisted of 23 five-point Likert scale (ranging from strongly disagree to strongly agree) questions aimed at evaluating the six constructs of the proposed research model in Figure 1. The self-administered questionnaire was designed based on the International Telecommunications Union (ITU) (ITU 2018) and the United Nations E-Government Survey Databases (United Nations 2016a) and adapted to the study in line with the proposed e-government use research model (Figure 1). The questionnaire was piloted with 10 respondents with prior experience in using e-government systems. Feedback from the pilot test was integrated into the final research instrument.

Data collection was administered over 8 weeks, covering Zimbabwe and Zambia. Structural equation modelling (SEM) (Kline 2011) using the IBM SPSS AMOS version 24 was used for validating the proposed model. The SEM allowed comprehensive testing of hypotheses using confirmatory factor analysis (CFA) to establish the significance of the relations among observed variables and latent variables of the proposed model of e-government utilisation as outlined in the following section.

Ethical consideration

An ethical clearance was obtained prior to fieldwork.

Results

Data cleaning and screening procedures

In line with Onwuegbuzie and Combs' (2011) suggestion, the data were scrutinised to firstly identify missing data, secondly to detect and deal with common method bias, and finally to detect and eliminate any possible outliers and univariate normality that could distort the findings.

Dealing with missing data

The pre-analysis phase of data analysis involved the screening of the survey instruments for item non-response and erroneous completion by the participants (Zhang & Yuan 2016). Out of the 550 distributed questionnaires, only 489 were suitable for the final data analysis. The rest were either incorrectly completed or had sections that were not completed, thus giving an overall response rate of 88.9%, which is considered more than adequate in line with the recommended acceptable response rate of 30% for any survey (Sekaran & Bougie 2010).

Dealing with common methods bias

Common method bias occurs when a measurement instrument (i.e. survey questionnaire) introduces some discrepancies in responses because of the way in which it is designed and phrased as opposed to the real dispositions of respondents (Podsakoff, MacKenzie & Podsakoff 2012). In this study, both the independent and dependent variables were measured using the same questionnaire and the same respondents. As a result, common method bias is possible. Two approaches were used in this study for testing and dealing with this: firstly, Harman's one-factor test to detect common method variance before executing exploratory factor analysis and, secondly, CFA using convergent and discriminant marker variables to detect common method variance. The rule of thumb for Harman's single-factor test is that the first major component's eigenvalue (percentage of variance) should be less than 50% to demonstrate the absence of the common method bias (Mudzana & Maharaj 2017; Podsakoff et al. 2012). The findings showed that when the first major component was extracted, only 17.85% of the variance was explained. This demonstrates that the remaining variance which was not extracted, explains a significant amount of the factors.

Dealing with univariate normality

Prior to conducting any statistical analysis, the data should first be tested for homogeneity to establish the data distribution for all the variables (Alshehri 2012). Here Pearson's first coefficient of skewness parameter test was used to establish univariate normality. However, the assessment of normality is sensitive to sample sizes and as such, Kim (2013) recommends the use of skewness and kurtosis for testing univariate normality for large sample sizes (i.e. $n > 300$). Kurtosis measures the 'relative peakedness or flatness of a distribution compared with the normal

distribution' (Čisar & Čisar 2010:96). Skewness measures the 'degree to which a statistical distribution is not in balance around the mean' (Čisar & Čisar 2010:97). According to Kim (2013), a perfectly skewed graph has a zero kurtosis and skewness values for a normally distributed histogram. Findings of this study show that the values for skewness range from –1.55050 to 1.20250; whilst that for kurtosis ranges from –0.56500 to 1.23175. Negative kurtosis and skewness values show a platykurtic distribution (flat-topped curve), whilst positive values indicate leptokurtic distribution (high peak) curve of the graph. Therefore, the kurtosis and skewness values for all the constructs in this study were within the acceptable ranges (i.e. ±3) (Kim 2013:53).

Descriptive analysis

The majority of the 489 valid responses were male (53%); 33% were aged between 26 and 35 years of age and 29% were between 36 and 45 years. More than half of the respondents (52%) indicated that they used the Internet on a daily basis whilst 42% used it one or more times per week. Forty-eight per cent of the respondents reported having used e-government once or twice per week, whilst 47% used it once or twice per month.

Measurement model analysis

Confirmatory factor analysis was used to establish the measurement model (testing discriminant and convergent validity of the measurement scales) and to determine how the model fits the collected data. As recommended by Hair et al. (2014), three tests (standardised factor loadings, construct reliability and average variance factor) were used to assess convergent validity in this study. The construct reliability results for this study are shown in Table 1. Standardised loadings show the level of association between scale items and an individual latent variable and only those latent variables above the minimum acceptable value of 0.50 (Hair et al. 2014) were loaded in Table 1. Construct reliability was done to ensure that the latent variables of each construct were internally consistent. Table 1 shows the reliability coefficients of all the constructs, ranging from 0.716 to 0.869, thus suggesting that the constructs were internally consistent because all coefficients were above the widely accepted minimum level of 0.70 (Hair et al. 2014).

The average variance extracted (AVE) was used to establish the convergent validity of the constructs, and all AVE values were above the minimum recommended threshold of 0.50 (Hair et al. 2014); thus reaffirming that the constructs of the proposed model explained more than 50% of variances of their underlying construct items.

Discriminant validity was carried out to establish and ensure that each construct of the study instrument was empirically unique from the rest of the constructs and characterises phenomena of interest in the structural equation model (Hair et al. 2014). AlKhatib (2013:276) suggests a rigorous method

TABLE 1: Reliability results.

Constructs	Standardised loadings	Construct reliability	AVE
Significant level	**≥0.50**	**≥0.70**	**≥0.50**
Perceived trust	-		
PT2	0.75	**0.845**	**0.647**
PT3	0.74		
PT4	0.90		
Perceived privacy	-		
PP1	0.68		
PP2	0.77	**0.869**	**0.561**
PP3	0.71		
PP4	0.89		
Perceived security	-		
PS1	0.79	**0.854**	**0.596**
PS3	0.83		
PS4	0.72		
Perceived risk	-		
PR1	0.82	**0.814**	**0.689**
PR2	0.79		
PR4	0.67		
Optimism bias	-		
OB1	0.92	**0.842**	**0.645**
OB2	0.71		
OB3	0.75		
Use behaviour	-		
USE1	0.78	**0.716**	**0.558**
USE2	0.71		

AVE, average variance extracted; PT, perceived trust; PP, perceived privacy; PS, perceived security; PR, perceived risk; OB, optimism bias; USE, use behaviour.

TABLE 2: Standardised construct correlation matrix.

	PT	PP	PS	PR	OB	USE
PT	0.800†	-	-	-	-	-
PP	0.269*	0.750†	-	-	-	-
PS	0.149**	-0.170**	0.770†	-	-	-
PR	-0.108*	-0.252**	-0.199*	0.830†	-	-
OB	0.154**	-0.068	0.455**	0.223**	0.800†	-
USE	0.371**	0.395**	-0.250**	-0.504*	0.486**	0.750†

PT, perceived trust; PP, perceived privacy; PS, perceived security; OB, optimism bias; USE, use behaviour.

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

†, values show the square roots of average variance extracted for each construct; all values below this diagonal line are correlation estimates for the constructs.

for computing discriminant validity in which the 'absolute values of correlations between the constructs' are compared with the square root of the AVE for that specific construct. The rule of thumb according to AlKhatib (2013) is that the square root of the AVE for that specific construct should always be greater than the AVE and all the correlations with all the other constructs. As illustrated in Table 2, the square roots (shaded in grey) were greater than the associated correlations for all the other constructs; thus there were no concerns regarding the discriminant validity. Therefore, the results in Tables 1 and 2 suggest that the CFA results provided acceptable discriminant and convergent validity for the construct scales of the questionnaire.

Structural model analysis

Following the validation of the model measurement, testing and validation of the overall fit of the structural model were pursued in this study, using a different set of fit indices.

The overall value of the chi-square (χ^2) was 459.82 with 230 degrees of freedom and with p-value < 0.05. A significant p-value (<0.05) shows that the absolute fit of the proposed model was not desirable. However, as the chi-square test for absolute model fit is too sensitive to sample size, Hooper, Coughlan and Mullen (2008) suggest the use of a more robust and satisfactory measurement, the chi-square over degrees of freedom. The chi-square over degrees of freedom for the proposed research model of this study was 1.69 and within the recommended 1 and 3 range (Kenny 2015). Along with the above two ratios, several fit indices for the model were reported. Descriptive fit indices are used to compare a specified model with a baseline model (sometimes referred to as an independent model) in order to prove the supremacy of the proposed model. To measure the overall model fit, several indices were used in this study – goodness-of-fit index, normed-fit index and comparative fit index, all of which should be equal to or greater than 0.90 (Albesher 2015). Other indices reported, were the index of fit and Tucker–Lewis index, which should have a value of 0.95 or above (Ugulu 2013). The adjusted goodness-of-fit index should be at or above 0.80, whilst the root-mean-square error of approximation should be below 0.08 to show good fit or below 0.05 to show excellent fit (Henseler et al. 2015; Steiger & Lind 1980). Table 3 shows that all indices were above the minimum recommended values – thus demonstrating a good fit of the proposed research model.

Path coefficient and hypothesis testing

Having established the structural model fit for the proposed model, this section examines the path coefficients of the latent variables in the constructs. Following Hair et al.'s (2014) recommendation that the parameter coefficient value be statistically significant (at $p < 0.05$ level) when its critical ratio (CR)/t-value for a standardised regression weight is greater than 1.96, all eight alternative hypotheses were significant (see Table 4). All critical ratios (CR)/t-value for the standardised regression weights were above the recommended 1.96 level. Figure 2 presents the structural path coefficient test results.

In all of the cases illustrated in Table 4, the null hypotheses were rejected. The following interpretations are presented:

- H_{1a}: Users were more likely to use G2C systems if they were confident about the privacy of their transactions.
- H_{2a}: A greater level of transactional privacy led to less perceived risk.
- H_{3a}: Improved trust in G2C systems leads to less perceived risk.
- H_{4a}: The more trust the user has in the system, the more likely he or she is to use it.
- H_{5a}: As perceived security increases, perceived risk decreases.
- H_{6a}: An increase in perceived security leads to increased use.
- H_{7a}: Greater perceived risk leads to decreased use.
- H_{8a}: Respondents who felt comfortable using G2C systems (more technically competent) felt less vulnerable using such systems and thus used them more.

Figure 2 shows that 81% of the discrepancies among the five endogenous constructs were explained by the use behaviour

TABLE 3: Structural model fit summary of the proposed model.

Absolute fit index	Recommended cut-off value	Final structural model
p	p-value < 0.05	0.001
χ^2	n/a	459.820
χ^2/df	1 < df < 3	1.690
df	df ≥ 0	230.000
GFI	≥0.90	0.942
AGFI	≥0.80	0.890
CFI	≥0.90	0.904
NFI	≥0.90	0.978
IFI	≥0.95	0.969
TLI	≥0.95	0.954
RMSEA	<0. 08 (good fit) or <0.05 (excellent fit)	0.032

GFI, goodness-of-fit index; AGFI, adjusted goodness-of-fit index; CFI, comparative fit index; NFI, normed-fit index; IFI, index of fit; TLI, Tucker–Lewis index; RMSEA, root-mean-square error of approximation.

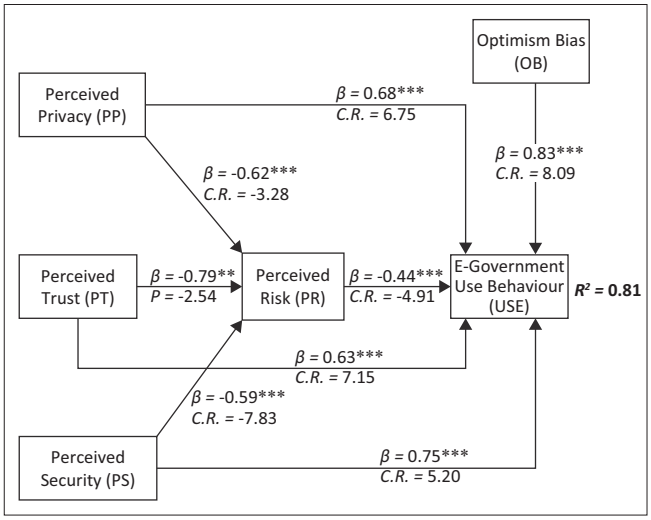

FIGURE 2: Structural model path coefficients.

TABLE 4: Path coefficient and hypothesis testing.

Hypothesis number	Hypothesised path	Estimate	SE	CR	β	p	Hypothesis supported by findings?
$H1_a$	PP → USE	0.81	0.12	60.75	0.65	***	Yes
$H2_a$	PP → PR	-0.59	0.18	-30.28	-0.62	***	Yes
$H3_a$	PT → PR	-0.60	0.24	-20.54	-0.79	0.02*	Yes
$H4_a$	PT → USE	0.50	0.07	70.15	0.63	***	Yes
$H5_a$	PS → PR	-0.47	0.06	-70.83	-0.59	***	Yes
$H6_a$	PS → USE	0.78	0.15	50.20	0.75	0.01**	Yes
$H7_a$	PR → USE	-0.51	0.01	-40.91	-0.44	***	Yes
$H8_a$	OB → USE	0.89	0.11	80.09	0.83	***	Yes

Estimate, standard regression weights/path estimates; SE, standard error; CR, critical ratio/t-value; p-value, significance level; PT, perceived trust; PP, perceived privacy; PS, perceived security; PR, perceived risk; OB, optimism bias; USE, use behaviour.

*, $p < 0.05$; **, $p < 0.01$; ***, $p < 0.001$.

of e-government systems. This shows that the proposed model has good predictive power (Hair et al. 2014) about the use behaviour of e-government systems in Zimbabwe and Zambia.

Discussion

This study investigated the extent to which privacy, security, trust, perceived risks and optimism bias influenced citizens' use behaviour of e-government systems in Zimbabwe and Zambia. To achieve this aim, this study proposed eight hypotheses to test the proposed model.

Some of the transactions performed by citizens (like e-filing of personal tax returns and payment of municipality bills) using e-government systems are sensitive and confidential and have strict deadlines that, if missed, could result in severe penalties. In such cases, citizens who felt that the e-government systems did not guarantee privacy to their transactions and could increase their vulnerability to risks were less motivated to use such systems when interacting with a government agency. In particular, this study found that privacy is a fundamental building block that determines whether e-government initiatives fail or succeed. Consistent with previous studies on e-government utilisation (Al Khattab et al. 2015; Alzahrani, Al-Karaghouli & Weerakkody 2016; Bwalya & Healy 2010; Cai Shuqin et al. 2016), findings of this study show that perceived privacy is negatively linked to perceived risk. The results also revealed that positive perceptions of privacy of personal data and transaction increase the utilisation of e-government systems. This finding concurs with findings of Singh and Sharma (2009), who found that privacy and confidentiality issues pose a huge challenge to the acceptance and use of e-government systems where sensitive information and decisions (as in e-voting and e-medicine) should never be divulged.

This study revealed that when citizens have a high level of trust in e-government systems, their perception of risk associated with the use of such systems tends to decrease. The opposite is equally true, high-risk perception leads to low trust in e-government systems. This was expected, given that the majority of the respondents in this study felt that there were inadequate operative legal structures in place to protect them from possible problems faced whilst transacting on e-government systems. Moreover, a significant number of participants felt that a lot should be done before they could trust e-government systems with their personal and confidential information. This finding is consistent with findings of prior studies (Basu 2004; Schaupp & Carter 2010) but inconsistent with Sharma (2014) and Zhou (2011), who found a positive relationship between trust and perceived risk. Citizens' trust was found to have a positive impact on use behaviour of e-government systems. A plausible explanation could be that when citizens become familiar with using electronic systems without encountering numerous challenges, chances are high that they tend to trust such systems and become motivated to keep on using them. Similarly, if citizens have a low perception of trust associated with the use of e-government systems, they are bound to trust such systems less. This finding concurs with findings of previous studies on e-government use (Al Khattab et al. 2015; Albesher 2015; Santhanamery & Ramayah 2016).

This study established a negative association between perceived security and perceived risk, implying that an increase in security features on e-government systems leads to low risk perceptions and vice versa. Robust security measures on e-government transactions mitigate fears associated with a potential loss by citizens. These findings disagree with results of previous studies (Oktem, Demirhan & Demirhan 2014; Shuqin et al. 2016; Zhao & Zhao 2010), which established a positive relationship between perceived security and risk perception; but they concur with Baganzi and Lau (2017) and Zafiropoulos et al. (2012). A plausible explanation for such differences in findings is that this study focused entirely on e-government users, most of whom could not be security savvy and as such, any security fears tend to raise risk perceptions. Citizens who regarded e-government systems as secure when interacting with a government agency were motivated to use such systems. However, these were not the only findings; Sharma (2015) established a positive correlation between perceived security and e-government adoption.

Perceived risk had a negative effect on use behaviour. Citizens who perceived e-government systems to be risky were less motivated to use such systems when engaging with government agencies. The results of this study agree with findings of earlier studies (Al Khattab et al. 2015; Almarashdeh & Alsmadi 2017; Schaupp & Carter 2010), which established that citizens who regard e-government systems to be risky tend to shun transacting over such systems and resort to an alternative medium. This implies that in order for e-government systems to gain the trust of citizens and become a major channel for accessing government services in the two countries, any risk issues and perceptions should be comprehensively addressed.

Optimism bias had a positive and significant effect on use behaviour. Despite having negative perceptions of the privacy, security and risk issues of e-government use, citizens who regarded themselves as more competent in using electronic systems compared to average users were more motivated and likely to use such systems. The results of this study are consistent with the empirical results of a study by Carlin (2016). A plausible explanation for these results is that as users become competent and familiar with using e-government systems, they do not regard themselves as susceptible to cybersecurity threats.

Implications for theory and practice

This study contributes to the existing corpus of literature by describing how cybersecurity issues (privacy, security, trust and risk) are affecting citizens' decisions to use e-government systems in Zimbabwe and Zambia. The

research has contributed to the body of knowledge on theory building by assimilating and testing four pertinent factors relating to cybersecurity and how optimism bias encourages citizens to keep on using such systems despite perceived risks. The findings draw attention to the fact that whilst citizens may consider the use of e-government systems as risky, trust in both the system and government entities is essential to encourage system utilisation. Moreover, the proposed model can be used as a springboard for future research direction and integrated with other existing models like the theory of acceptance and use of technology (UTAUT), thus broadening the understanding of factors affecting e-government utilisation. This study has strong implications for practice. It underscores that citizens' utilisation levels of e-government systems are significantly affected by their lived experiences and perceptions of privacy, security and trust in a government agency, the e-system itself and legal structures in place to protect users. Therefore, privacy, security and trust are fundamental ingredients that neutralise perceived risks and dictate the degree of success or failure of e-government systems. Optimism bias works best when citizens have established some level of trust in the government and the privacy and security of e-government systems. This study reveals the pitfalls of e-government adoption and utilisation by citizens if privacy and security concerns are perceived as inadequate. Hence, implications for the design and implementation of e-government systems are that governments should adopt people-driven initiatives in which citizens' and governments' inputs play an equal role towards any new e-government initiative.

Conclusion

This research investigated the effect of the latent variables of privacy, security, trust, perceived risk and optimism bias on the utilisation of e-government systems in Zimbabwe and Zambia. A conceptual model integrating these latent variables into a behavioural-related model to determine their effect on e-government utilisation was developed based on the NICE-CMM, NIST Cybersecurity Framework, UTAUT2 and the ADM theory and was presented. Survey data for testing the proposed model were collected from 489 e-government users in Zimbabwe and Zambia. A key finding was that security concerns for the majority of e-government users are based on sentiment because they are not well versed with the particulars of security. To encourage adoption, the government should work to reduce any uncertainties associated with the use of e-government and build citizens' trust. Perceived privacy, perceived security and perceived trust were found to be negatively associated with perceived risk. Perceived trust, perceived privacy, perceived security and optimism bias were positively associated with use behaviour. Future research work should investigate the direct impact of privacy, security and trust in citizens' intention (focusing on non-users) to adopt e-government systems in Zimbabwe and Zambia.

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

This article arises out of the research conducted by W.M.M. for his doctoral thesis, under the supervision of M.S.M.

References

Albesher, A., 2015, 'Trust as a source of long-term adoption of e-government', PhD Thesis, Brunel University, London.

Al Khattab, A., Al-Shalabi, H., Al-Rawad, M., Al-Khattab, K. & Hamad, F., 2015, 'The effect of trust and risk perception on citizen's intention to adopt and use e-government services in Jordan', *Journal of Service Science and Management* 8, 279–290. https://doi.org/10.4236/jssm.2015.83031

AlKhatib, H., 2013, 'E-government systems success and user acceptance in developing countries: The role of perceived support quality', PhD Thesis, Brunel University, London, United Kingdom.

Almarashdeh, I. & Alsmadi, M.K., 2017, 'How to make them use it? Citizens acceptance of m-government', *Applied Computing and Informatics* 13(2), 194–199. https://doi.org/10.1016/j.aci.2017.04.001

Alsaghier, H., Ford, M., Nguyen, A. & Hexel, R., 2009, 'Conceptualising citizen's trust in e-government: Application of Q methodology', *Electronic Journal of e-Government* 7(4), 295–310.

Alshehri, M.A., 2012, 'Using the UTAUT model to determine factors affecting acceptance and use of E-Government services in the United Kingdom of Saudi Arabia', PhD Thesis, Griffith University.

Al-Zoubi, R.B.K., 2008, 'Public centric e-governance in Jordan', *Journal of Information, Communication and Ethics in Society* 6(4), 317–333.

Alzahrani, L., Al-Karaghouli, W. & Weerakkody, V., 2016, 'Developing citizens' trust towards successful adoption of e-government: An empirical study from Saudi Arabia', *Academy of Contemporary Research Journal* 5(2), 9–15.

Anthopoulos, L., Reddick, C.G., Giannakidou, I. & Mavridis, N., 2016, 'Why e-government projects fail? An analysis of the healthcare.gov website', *Government Information Quarterly* 33, 161–173. https://doi.org/10.1016/j.giq.2015.07.003

Bansal, G., Zahedi, F.M. & Gefen, D., 2010, 'The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online', *Decision Support Systems* 49(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Baganzi, R. & Lau, A.K.W., 2017, 'Examining trust and risk in mobile money acceptance in Uganda', *Sustainability* 9, 1–22.

Basu, S., 2004, 'E-government and developing countries: An overview', *International Review of Law Computers & Technology* 18(1), 109–132. https://doi.org/10.1080/13600860410001674779

Bracha, A. & Brown, D.J., 2012, 'Affective decision making: A theory of optimism bias', *Games and Economic Behaviour* 75(1), 67–80. https://doi.org/10.1016/j.geb.2011.11.004

Bwalya, K.J., 2017, 'Determining factors influencing e-government development in the developing world: A case study of Zambia', *Journal of E-Government Studies and Best Practices*, 2017, Article ID 143795. https://doi.org/10.5171/2017.143795

Bwalya, K.J. & Healy, M., 2010, 'Harnessing e-government adoption in the SADC region: A conceptual underpinning', *Electronic Journal of e-Government* 8(1), 23–32.

Cai Shuqin, B.H.M., Mastoi, A.G., Gul, N. & Gul, H., 2016, 'Evaluating citizen e-satisfaction from e-government services: A case of Pakistan', *European Scientific Journal* 12(5), 346–370.

Carlin, J.P., 2016, 'Detect, disrupt, deter: A whole-of-government approach to national security cyber threats', *Harvard National Security Journal* 7, 391–436.

Čisar, P. & Čisar, S.M., 2010, 'Skewness and kurtosis in function of the selection of network traffic distribution', *Acta Polytechnica Hungarica* 7(2), 95–106.

Colesca, S.E., 2009, 'Understanding trust in e-government', *Inzinerine Ekonomika-Engineering Economics* 3, 7–15.

Creswell, J.W., 2014, *Research design: Qualitative, quantitative and mixed methods approaches*, 4th edn., Sage, London, England.

Ewurah, S.K.M., 2017, 'The concept of e-government: ICT policy guidelines for the policymakers of Ghana', *Journal of Information Security* 8, 106–124. https://doi.org/10.4236/jis.2017.82008

Fakhoury, R. & Baker, D.S., 2016, 'Governmental trust, active citizenship, and e-government acceptance in Lebanon', *Journal of Leadership, Accountability and Ethics* 13(2), 36–52.

Gelo, O., Braakmann, D. & Benetka, G., 2008, 'Quantitative and qualitative research: Beyond the debate', *Integrative Psychological and Behavioural Science* 42(3), 266–290. https://doi.org/10.1007/s12124-008-9078-3

Hair, J.F., Black, W.C., Babin, B.J. & Anderson, R.E., 2014, *Multivariate data analysis*, 7th edn., Pearson Publishers, Harlow, Essex.

Hassan, R.G. & Khalifa, O.O., 2016, 'E-government – An information security perspective', *International Journal of Computer Trends and Technology* 36(1), 1–9. https://doi.org/10.14445/22312803/IJCTT-V36P101

Henseler, J., Ringle, C.M. & Sarstedt, M., 2015, 'A new criterion for assessing discriminant validity in variance-based structural equation modelling', *Journal of the Academy of Marketing Science* 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hooper, D., Coughlan, J. & Mullen, M., 2008, 'Structural equation modelling: Guidelines for determining model fit', *Electronic Journal of Business Research Methods* 6(1), 53–60.

International Telecommunications Union [ITU], 2012, *Understanding cybercrime: Phenomena, challenges and legal response*, viewed 08 November 2017, from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

International Telecommunication Union [ITU], 2018, *Statistics 2018*, viewed 20 February 2018, from http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Kenny, D.A., 2015, *Measuring model fit*, viewed 25 February 2018, from http://davidakenny.net/cm/fit.htm.

Kim, H.Y., 2013, 'Statistical notes for clinical researchers: Assessing normal distribution using skewness and kurtosis', *Restorative Dentistry & Endodontics* 38(1), 52–54. https://doi.org/10.5395/rde.2013.38.1.52

Kline, R.B., 2011, *Principles and practice of structural equation modeling*, The Guilford Press, New York.

Majdalawi, Y.K.H., Almarabeh, T., Mohammad, H. & Quteshate, W., 2015, 'E-government strategy and plans in Jordan', *Journal of Software Engineering and Applications* 8, 211–223. https://doi.org/10.4236/jsea.2015.84022

Mistry, J.J. & Jalal, A., 2012, 'An empirical analysis of the relationship between e-government and corruption', *The International Journal of Digital Accounting Research* 12(6), 145–176. https://doi.org/10.4192/1577-8517-v12_6

Mudzana, T. & Maharaj, M., 2017, 'Toward an understanding of business intelligence systems success: A South African study', *The Electronic Journal Information Systems Evaluation* 20(1), 24–38.

Munyoka, W. & Maharaj, M., 2017., 'Understanding e-government utilisation within the SADC', *IST-Africa 2017 Conference Proceedings*, 31 May–02 June 2047, Windhoek, Namibia.

National Institute of Standards and Technology (NIST), 2018, *Framework for improving critical infrastructure cybersecurity*, (v.1.1), April 16, 2018, NIST Research Library, Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.04162018

Oktem, M.K., Demirhan, K. & Demirhan, H., 2014, 'The usage of e-governance applications by higher education students', *Kuram Ve Uygulamada Egitim Bilimleri* 14(5), 1925–1943.

Onwuegbuzie, A.J. & Combs, J.P., 2011, 'Data analysis in mixed research: A primer', *International Journal of Education* 3(1), 1–25. https://doi.org/10.5296/ije.v3i1.618

Papadomichelaki, X. & Mentzas, G., 2012, 'e-GovQual: A multiple-item scale for assessing e-government service quality', *Government Information Quarterly* 29, 98–109. https://doi.org/10.1016/j.giq.2011.08.011

Pathak, R.D. Singh, G., Belwal, R., Naz, R. & Smith, R.F.I., 2008, 'E-governance, corruption and public service delivery: A comparative study of Fiji and Ethiopia', *Journal of Administration & Governance* 3(1), 65–79.

Podsakoff, P.M., MacKenzie, S.B. & Podsakoff, N.P., 2012, 'Sources of method bias in social science research and recommendations on how to control it', *Annual Review of Psychology* 63(1), 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Ramli, R.M., 2017, 'E-government implementation challenges in Malaysia and South Korea: A comparative study', *Electronic Journal of Information Systems in Developing Countries* 80(7), 1–26. https://doi.org/10.1002/j.1681-4835.2017.tb00591.x

Santhanamery, T. & Ramayah, T., 2016, 'The effect of trust in the system and perceived risk in influencing continuance usage intention of an e-government system', *Journal of Applied Environmental and Biological Sciences* 6(3), 7–18.

Schaupp, L.C. & Carter, L., 2010, 'The impact of trust, risk and optimism bias on e-file adoption', *Information Systems Frontier* 12, 299–309. https://doi.org/10.1007/s10796-008-9138-8

Sekaran, U. & Bougie, R., 2010, *Research methods for business: A skill building approach*, 5th edn., John Wiley & Sons, New Jersey, NY.

Shalhoub, Z.K., 2006, 'Trust, privacy, and security in electronic business: The case of the GCC countries', *Information Management & Computer Security* 14(3), 270–283. https://doi.org/10.1108/09685220610670413

Shareef, M., Kumar, V., Kumar, U. & Dwivedi, Y.K., 2011, 'eGovernment adoption model (GAM): Differing service maturity levels', *Government Information Quarterly* 28, 17–35. https://doi.org/10.1016/j.giq.2010.05.006

Sharma, G., 2014, 'E-government, e-participation and challenging issues: A case study', *International Journal of the Computer, the Internet and Management* 22(1), 23–35.

Sharma, S.K., 2015, 'Adoption of e-government services: The role of service quality dimensions and demographic variables', *Transforming Government: People, Process and Policy* 9(2), 207–222. https://doi.org/10.1108/TG-10-2014-0046

Shuqin, B.H.M., Mastoi, A.G., Gul, N. & Gul, N., 2016, 'Evaluating citizen e-satisfaction from e-government services: A case of Pakistan', *European Scientific Journal* 12(5), 346–370.

Singh, A.J. & Sharma, V., 2009, 'E-governance and e-government: A study of some initiatives', *International Journal of E-Business and E-Government Studies* 1(1), 1–14.

Singh, S. & Karaulia, D.S., 2011, 'E-governance: Information security issues', *Proceedings of the International Conference on Computer Science and Information Technology,* Pattaya, Thailand, 17–18 December.

Steiger, J.H. & Lind, J.C., 1980, *Statistically based tests for the number of common factors*, The annual meeting of the Psychometric Society, Iowa City, IA.

The World Bank, 2016, *Digital dividends: World development report*, The World Bank, Washington, DC.

Ugulu, I., 2013, 'Confirmatory factor analysis for testing validity and reliability of traditional knowledge scale to measure university students' attitudes', *Educational Research and Reviews* 8(16), 1399–1408.

United Nations, 2016a, *UN e-government knowledge database 2016*, viewed 15 December 2017, from https://publicadministration.un.org/egovkb/en-us/#.WFFeEbJ97IU.

United Nations, 2016b, *E-Government survey 2016, e-government in support of sustainable development*, United Nations, New York, NY.

US Department of Homeland Security., 2014, *Cybersecurity Capability Maturity Model*, White Paper (v.1), August 04, 2014. Washington, DC.

Venkatesh, V., Thong, J.Y.L. & Xu, X., 2012, 'Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology', *MIS Quarterly* 36(1), 157–178. https://doi.org/10.2307/41410412

Weinstein, N.D., 1980, 'Unrealistic optimism about future life events', *Journal of Personality & Social Psychology* 39, 806–820. https://doi.org/10.1037/0022-3514.39.5.806

Xu, H., Teo, H.H., Tan, B.C.Y. & Agarwal, R., 2009, 'The role of push-pull technology in privacy calculus: The case of location-based services', *Journal of Management Information Systems* 26(3), 135–173. https://doi.org/10.2753/MIS0742-1222260305

Zafiropoulos, K., Karavalisis, I. & Vrana, V., 2012, 'Assessing the adoption of e-government services by teachers in Greece', *Future Internet* 4, 528–544. https://doi.org/10.3390/fi4020528

Zhang, Z. & Yuan, K., 2016, 'Robust coefficients alpha and omega and confidence intervals with outlying observations and missing data: Methods and software', *Educational and Psychological Measurement* 76(3), 387–411. https://doi.org/10.1177/0013164415594658

Zhao, J. & Zhao, S., 2010, 'Opportunities and threats: A security assessment of state e-government websites', *Government Information Quarterly* 27, 49–56. https://doi.org/10.1016/j.giq.2009.07.004

Zhou, T., 2011, 'The impact of privacy concern on user adoption of location-based services', *Industrial Management & Data Systems* 111(2), 212–226. https://doi.org/10.1108/02635571111115146