Journal of Systems and Information Technology

The role of trust in enhancing Internet use in a high-risk society
Almamy Touray Taina Savolainen Airi Salminen Erkki Sutinen Yue Dai

The role of trust in enhancing Internet use in a high-risk society

Almamy Touray
Department of Computer Science & Information Systems, University of Jyväskylä, Jyväskylä, Finland
Taina Savolainen
Business School, University of Eastern Finland, Joensuu, Finland
Airi Salminen
Department of Computer Science & Information Systems, University of Jyväskylä, Jyväskylä, Finland, and
Erkki Sutinen and Yue Dai
School of Computing, University of Eastern Finland, Joensuu, Finland

Received 22 September 2014
Revised 15 March 2015
Accepted 16 March 2015

Abstract

Purpose – This paper aims to determine the key trust antecedents that influence Internet users' trust level toward Internet service providers (ISPs) in a high-risk society. It also investigates trust-building process, major causes of its violation, their potential implications and restoration.

Design/methodology/approach – A mixed-method approach was used in collecting data in Kenya in 2014 by using questionnaire and interview techniques. The former was administered to 250 (with 81 per cent response rate) randomly selected Internet users at Kenyatta University while the latter focused on key decision-makers from four randomly selected ISPs in Nairobi.

Findings – The results show that Internet users' perceptions of ISPs' ability to be trusted in Kenya depend more on their competence in terms of service delivery (ability) and desire to protect users (benevolence) than upholding acceptable standards (integrity). The results also indicate a lack of trust manifested in poor communication and greed for profit among ISPs as major causes of trust violation.

Originality/value – This paper proposes two frameworks that can enhance Internet use by providing a better understanding of trust in a high-risk society.

Keywords Africa, Internet use, High-risk society, Kenya, Developing countries, Mixed-method, Revised trust framework, Risk mitigation, Trust

Paper type Research paper

We are grateful to the Nokia Foundation, the Finnish Science Foundation for Economics and Technology (KAUTE), the University of Jyväskylä's graduate school of Computing and Mathematical Sciences (COMAS) and the department of Computer Science and Information Systems for jointly sponsoring this research. We would also like to extend our immense gratitude to the host institutions, Kenyatta University and Telecommunications Service Provider Association of Kenya (TESPOK). Last but not least, we would like to thank Mark and his family for their support in a number of practical arrangements during the entire data collection period in Kenya.

Journal of Systems and Information Technology
Vol. 17 No. 2, 2015
pp. 141-166

1328-7265
DOI 10.1108/JSIT-09-2014-0066

1. Introduction

Many researchers (Kyobe, 2011a; Avgerou, 2008; Bankole *et al.*, 2011; Sahey and Avgerou, 2002 and Walsham and Sahey, 2006) perceive information and communication technology (ICT) as a platform for development. However, it is imperative to acknowledge that the Internet is one of the most important innovations that has transformed the ICT domain. It is one of the technologies required to support information processing to execute applications and deliver services (Leahy and Yermis, 2003; Mofleh *et al.*, 2008 and Raji *et al.*, 2006). The Internet is also a tremendous, undisputed force for economic growth and social change (Dalberg Survey Report, 2013). However, its potential is still largely untapped particularly in Sub-Saharan Africa (Dalberg Survey Report, 2013), and access to the technology in Africa as a whole is progressing at a limited pace (Alshameri and Banjura, 2014). For instance, Africa's number of Internet users is just six per every 100 inhabitants (International Telecommunication Union [ITU], 2013), which is far less than the world average of about 46 per cent. In addition, the number of households with Internet is just 7 per cent (ITU, 2013), and this figure is estimated to increase in 2014 by just 4 per cent (ITU, 2014). Furthermore, Africa's Internet penetration rate in 2014 is 19 per cent (ITU, 2014), which is also far less than the corresponding world average of about 49 per cent. These statistics demonstrate a major obstacle in terms of Internet use on the continent.

It is imperative to briefly define two important key concepts that are used in this paper, namely, developing country and high-risk society. A *developing country* has lesser income and purchasing power, as well as insufficient basic amenities compared to the developed world. Essentially, we consider a *high-risk society* as an environment where there is a great deal of distrust. It is important to note that other areas of high risk exist in circumstances of political instability, famine, natural disasters, etc. However, we focus on high-risk society in the context of trust building. We chose Kenya as our case country due to its location in a high-risk region (African Development Bank [ADB], 2013).

Trust is a vital element that has the potential to overcome the digital drought in Africa while distrust is one factor that impedes Internet use in developing countries (Popola, 2013). Building trust can, therefore, help enhance digital adoption in Africa, the significance of which is widely recognized (Zeffane, 2010). Trust can impact one's sense of security which is a critical issue in today's digitalized world (Six, 2005). It develops incrementally over time and involves interaction between actors such as Internet service providers (ISPs) and users (Connell *et al.*, 2003). Trust can overcome privacy concerns because people are most often guarded about their privacy when they lack trust in others (World Economic Forum, 2011), and it is important during situations of perceived high risk (Johnson *et al.*, 2003 and Joubert and Van Belle, 2013) such as on the African continent (African Development Bank [ADB], 2013). It is vital to note that trust is combined with risk, as the former involves taking risks and making oneself vulnerable to trust placed in others (Xu and Ba, 2003).

Evidence suggests that the conduct of service providers is one reason that influences consumers' decision to use Web-based applications (McKnight *et al.*, 1998). They indicated that trust plays a central role in helping consumers overcome perceived risk and insecurity. It can optimize service providers' chances of retaining their customers (Casielles *et al.*, 2005). An additional study shows that societies which exhibit high trust do better economically (Fukuyama, 1995). Researchers (Serva *et al.*, 2005) highlight the

importance of a deeper contextual consideration in trust theory development. Trust research often focuses more on organizations, managers, individuals or work groups without paying attention to individuals' cultural background (Costa, 2003). It is, however, a fundamental social process which differs across cultures (Fulmer and Gelfand, 2012). They stressed the need for universal and culture-specific aspects of trust and local practices in future research.

Previous studies on trust have been criticized for either failing to effectively conceptualize trust or describing it in a relatively narrow scope (Grabner-Krauter and Kalushaha, 2003). According to the World Economic Forum report (2011), little is known about the values and attitudes of Internet users around the world. We cannot assume that globalization leads to the homogenization of world cultures which makes it important to acknowledge the multicultural and multidimensional nature of online behavior (WEF, 2011). Researchers (Joubert and Van Belle, 2013) highlighted the importance of investigating consumers' ability to trust service providers. Therefore, the context of this paper will strengthen our understanding of trust from a different perspective. This study investigates trust toward ISPs in the context of a high-risk society such as Kenya. Our goal is to examine trust antecedents that were identified by prior researchers (Mayer *et al.*, 1995; Popola, 2013; Cho *et al.*, 2007 and Thaw *et al.*, 2009). Furthermore, we want to explore the major causes of trust violation, its potential implications and restoration in the Kenyan context. Based on our findings, we will propose two frameworks to increase understanding of trust in a high-risk society and thereby provide support to enhance Internet use. Essentially, we aim to address the following research questions:

RQ1. What are the key trust antecedents that influence Internet users' trust level toward ISPs in a developing country?

RQ2. What are the major factors in trust building, causes of its violation, potential implications and its restoration in terms of Internet adoption in a developing country?

The remainder of this paper is organized as follows: Section 2 covers the theoretical background of the study, and Section 3 presents the research methodology. Sections 4 and 5 present the quantitative and qualitative results, respectively. Section 6 entails a brief discussion on the theme of trust, while Section 7 summarizes the study's key results, its implications, states its main limitations and indicates the direction of future research.

2. Theoretical background

Trust is a vital aspect of our everyday life. There is a growing literature on the connections between ICTs such as the Internet, trust and human development (Kuriyan *et al.*, 2010 and Salgado, 2012). As a baby, we are initiated to trust through a deep and abiding faith that emerges from the relationship with those who care for us (Rath, 1972). Trust is a multifaceted and multidisciplinary issue that has been widely studied (Popola, 2013; Blanchard *et al.*, 2011; Cho *et al.*, 2007 and Thaw *et al.*, 2009). It involves several theoretical approaches, definitions, factors and models (Rousseau *et al.*, 1998). In the field of psychology, trust is examined in terms of cognition, affection and behavior. A willingness to be vulnerable is still emphasized as the key element. In organizational context, trust develops from interaction and reciprocal activity between individuals and

within groups. It is seen as an important intangible asset in organizations (Savolainen and Lopez-Fresno, 2013), for example, where trust forms a basis for cooperation. Trust has recently been identified as one of the most frequently examined constructs in the organizational literature (Burke *et al.*, 2007). It has been defined in many ways, yet the concept itself remains somewhat unclear (McEvily *et al.*, 2003). Trust is generally defined as:

> […] the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party (Mayer *et al.*, 1995, p. 712).

In other words, trust can be seen as a person's assessment of one's ability to be trusted. Mayer's model considers the formation of trust between actors in a relational context. Trust formation evolves overtime through repeated interactions and communication between trustor(s) and trustee(s).

The aforementioned definition of trust covers person-to-person and person-to-organization relationships (Mayer *et al.*, 1995). The three dimensions of ability, benevolence and integrity have been proposed by Mayer *et al.* (1995) as the key elements of trust. They are widely researched in fields such as psychology, management and leadership as well as IS/ICT (Zeffane, 2010; Savolainen and Häkkinen, 2011; Grabner-Krauter and Kalushaha, 2003 and Das and Teng, 2001). Researchers (Mayer *et al.*, 1995) assert that a trustor's level of trust and perceived risk will affect his or her risk-taking behavior. Risk is a vital element in their model of trust, as trust essentially refers to a willingness to assume risk (Mayer *et al.*, 1995). Studies have shown that once a trustor has received information about a trustee, the perception to trust wanes and the trusting behavior depends on the intent to trust (Davis, 1999; Mayer *et al.*, 1995 and Gill *et al.*, 2005). The research framework of this paper is adapted from the trust model proposed by Mayer *et al.* (1995). It focuses on the antecedents that lead to the development of one's intention to trust, namely, ability, benevolence and integrity (Figure 1):

- *Ability*: The competence level of the trustee (Das and Teng, 2001). Williams (2001) defines competence as "[…] [a] set of skills […] that allows [one] to perform in some area". Trusting another party depends on the trustor's perception that the trustee possesses ability or competence (Davis *et al.*, 2000). Researchers further highlight that ability is positively related to one's intention to trust (Gill *et al.*, 2005).
- *Benevolence*: The extent to which the trustor perceives that the trustee intends to do good to the trustor in a relationship (Mayer *et al.*, 1995 and Williams, 2001). In

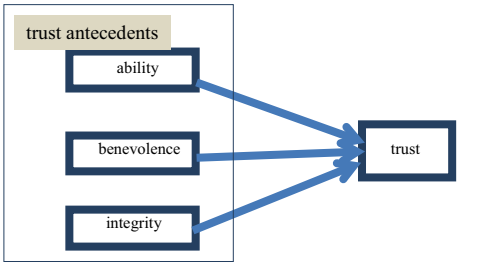

Figure 1.
Research framework

other words, benevolence entails a responsibility or desire to care for or protect another party.

- *Integrity*: The belief that parties (for instance, a trustor and trustee) will adhere to a set of acceptable standards, principles or values (Mayer *et al.*, 1995). A high degree of integrity is perceived as a positive trait in an individual (Audi and Murphy, 2006) and as a business asset (Koehn, 2005).

In this paper, each survey construct in Figure 1 is measured by three items (ability: AB1, AB2 and AB3; benevolence: BE1, BE2 and BE3; and integrity: IN1, IN2 and IN3), as shown in Figure 2. Furthermore, three additional items TR1, TR2 and TR3 are included in Figure 2 to examine Internet users' level of trust toward ISPs in Kenya.

3. Research methodology

This research uses a mixed-method approach that uses both quantitative and qualitative data (Green, 2007). A survey method is used in collecting quantitative data. This method has a particular purpose in producing scientific knowledge compared to the qualitative method. A survey method has precise procedures which, when followed closely, yield valid and easily interpretable data and reliable research findings that provide possible explanations and generalizations (Pinsonneault and Kraemer, 1993). Survey design has three distinct characteristics (Glasow, 2005). First, the phenomena to be studied should examine the relationship among variables. Second, the data should be collected from people. Finally, survey research should represent a selected portion of the population. The scope of a survey is determined by independent and dependent variables a researcher considers. It is also required to have a predicate model that depicts the expected relationship among variables (Glasow, 2005). The aforementioned characteristics of survey research make it an appropriate choice for this study. We strived in as much as possible to adhere to the guidelines in designing and implementing survey research (Glasow, 2005). A qualitative method was used as a complementary source of data collection. This approach is effective in obtaining culturally specific information about the values, opinions, behaviors and social contexts of a particular population (www.ccs.neu.edu). It is stated that "Not everything that can be counted

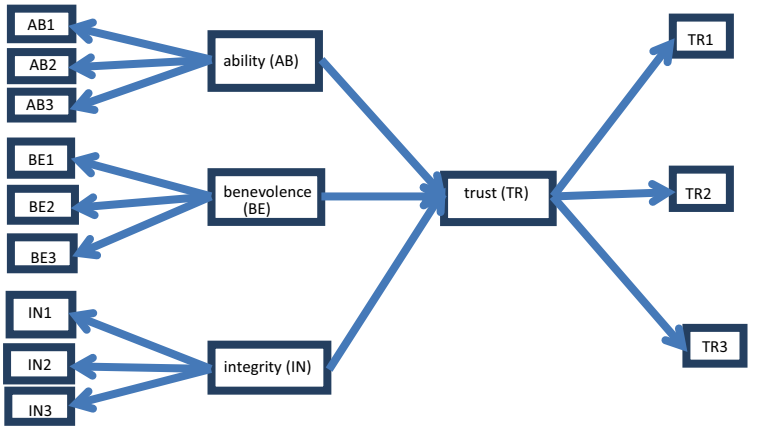

Figure 2.
Detailed research framework

counts, and not everything that counts can be counted" (Albert Einstein, quoted in Linder and Santiso, 2003, p. 2). In other words, the qualitative method helped us to get answers to questions about what, how and why aspects of this study.

3.1 Case context

Kenya is located in Eastern Africa bordering the Indian Ocean between Somalia and Tanzania. It shares borders with Ethiopia, South Sudan and Uganda. Kenya is the 49th largest country in the world by area spanning a total of 580,367 square kilometers (www.cia.gov). The country has a maternal mortality rate of 360 deaths per 100,000 live births and an infant mortality of 40.71 deaths per 1,000 live births (www.cia.gov). The average life expectancy in the country is 63.52 years (62.06 for male and 65.01 for female). It is estimated that about 6.1 per cent of Kenyans are living with HIV/AIDS (CIA, 2012), making it the fourth most affected nation in the world. The country has an average literacy rate of 87.4 per cent (90.6 of males and 84.2 of females) among those ages 15 and older (www.cia.gov).

3.2 Data collection

The data collection was conducted from March 3rd to March 29th, 2014 in Nairobi, Kenya. Kenyatta University (KU) and Telecommunications Service Provider Association of Kenya (TESPOK) were the host institutions during the survey period. It must be acknowledged that no statistical method was used in selecting the case university; rather, it was intentionally chosen based on positive feedback during the research design phase. However, a statistical approach was used in selecting both the research population and the participants (Figure 3). Prior to conducting the survey at KU, the main author requested formal permission from the Vice Chancellor (VC) of the university. Upon approval, the VC formally informed the deans of the six randomly selected faculties to seek the consent of both staff and students as research participants. The selected faculties were Engineering, Business Studies, Education, Economics, Applied Science and Hospitality and tourism. In addition, a personal follow-up was conducted by the main author of this paper. The quantitative data and part of the qualitative data for this study are collected from respondents from the aforementioned six faculties at KU.

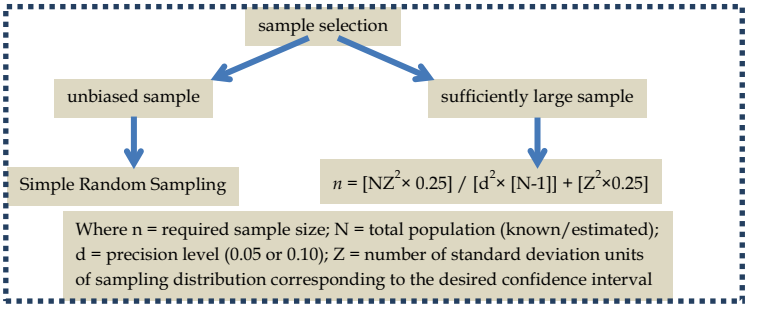

Figure 3.
Sampling approach

Source: Adapted from "Air University Sampling and Surveying Handbook" (2002)

The data collection process was conducted systematically as follows: we first determined the estimated number of potential participants in KU. An acceptable number of participants that would be statistically significant was determined based on the concept of a sufficiently large sample using the formula presented in Figure 3. The deans of each of the participating faculties nominated five research assistants to help the first author in collecting the required data. As the number of potential participants was more than required, a simple random sampling approach was conducted to determine the eventual research participants. Each one of them was given a questionnaire to complete within a week. Appendix 1 depicts the detailed survey questionnaire that was given to each research participant.

Similarly, the participants for the interviews were drawn from five randomly selected ISPs. They include Xtranet, Bandwidth and Cloud Services, Liquid Telecom, Wanachi Group and Jamii Telecom. Unfortunately, one of the ISPs decided to withdraw from the research at the last moment which made it impossible to find a replacement. To seek interview participants' consent, a formal written request was sent to the chief executive officers (CEOs) of the randomly selected ISPs from the CEO of the TESPOK on behalf of the first author. TESPOK and KU were research co-hosts for this study. The main participants at the ISP level were key decision-makers like CEOs. In a situation where we were unable to interview a CEO, he/she identified another senior officer. For each interview session, the first author was accompanied and assisted by the Communication Manager of TESPOK who asked respondents questions while the first author took field notes. Each interview lasted between about 30 to 90 minutes and was tape recorded. The interview questions are shown in Appendix 2.

3.2.1 Quantitative data. The quantitative data collection focuses on Internet users' perceived level of trust of ISPs and the amount of risk they are willing to take in terms of service delivery from ISPs. The age distribution of our respondents in years ranges from less than or equal to 20 up to 60, as shown in Table I. We used a closed-form questionnaire based on a five-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = neither agree nor disagree; 4 = agree; and 5 = strongly agree). The questionnaire used in the survey comprised of three distinct sections: demographic information, trust

Age range (in years)	Gender		Total no. of participants
	Female	Male	
≤20	17	7	24
21-25	34	69	103
21-25	No specified gender		1
26-30	7	5	12
31-35	12	10	22
36-40	6	8	14
41-45	8	12	20
41-45	No specified gender		1
46-50	0	0	0
51-55	1	0	1
56-60	1	0	1
≥61	No specified gender		1
No demographic information provided	No specified gender		2
Total number of participants	86	111	202

Table I.
Respondents' profile

antecedent and risk mitigation (Appendix 1). We used two important strategies in determining our sample size that truly reflect the target population of the study. The first was an unbiased sample and the second was a sufficiently large sample. The first strategy was achieved by using a simple random sampling technique on the target population. The statistical formula (Figure 3) was used to ensure that the second strategy could be attained. The risk related to sample size determination is specified by two interrelated factors, namely, the confidence level and the precision (or reliability) range (Air University Sampling and Surveying Handbook, 2002). To minimize risk, we choose a 95 per cent confidence level with a Z value of 1.96 and a 0.10 precision level. This enabled us to determine our sample size that will better represent the target population. The survey respondents' demographic information is depicted in Table I.

3.2.2 Qualitative data. By applying a qualitative approach, our aim was to deepen the understanding of the role of trust among key decision-makers from participating ISPs and Internet users. The role of a qualitative approach is to make the data rich and allow deeper interpretations than a quantitative approach would allow. In consideration of the cultural context and environment of data gathering in this study, the qualitative data can be considered especially valuable and rare due to access and collection challenges not to mention interactive interview sessions. The qualitative data were gathered using an interview method and open-ended questions which correspond to the aim of this study (see Section A.3 of Appendix 1 and interview questionnaire in Appendix 2). It is important to highlight that this study utilized only the themes and questions of the interview questionnaire that are marked asterisks. The affected themes are trust in Internet diffusion, trust building and maintenance and distrust, trust breach and restoring trust. We conducted four interviews with key decision-makers from the participating ISPs selected at random. The interview participant included a CEO, director, general manager and manager. We chose to deliberately omit the interviewees' names and their institutional affiliations for security reasons. These terms were agreed upon between the main author and interviewees prior to each interview session. The data from the four interviews and responses from Section A.3 of the survey questionnaire enabled us to identify how to build trust, major causes of distrust, its potential implications and how to restore trust.

3.3 Data analysis

The data analysis approach in this paper also follows mixed-method approach consisting of two phases: analyses of quantitative and qualitative data. The former uses exploratory factor analysis that helped us to identify the trust antecedents toward ISPs. Sampling adequacy of the quantitative data to justify the use of factor analysis was determined using the Kaiser–Meyer–Olkin (KMO) test. For factor analysis to work, some relationships are needed between the variables (Field, 2005). This was examined by using the Bartlett's test of sphericity. The internal reliability of our constructs was also verified by computing Cronbach's alpha value. The factor analysis method was used to check for construct validity (Kerlinger, 1986). Content validity (Nunnally, 1978) is supported by the literature review which helped us to develop our research framework. For the qualitative data, we manually transcribed all interview data based on transcription schemes of direct tape recording (Miles and Huberman, 1987). Content analysis (Strauss, 1987 and Eriksson and Kovalainen, 2008) was used to analyze the interview data and Section A.3 of the survey questionnaire which helped us to interpret

the qualitative data. These two schemes helped us to identify how to build trust, the major causes of distrust, its potential implications and how to restore trust. More importantly, they enabled us to develop a risk-mitigation framework for a high-risk society.

4. Quantitative results

As mentioned above, 202 valid questionnaires were returned by survey respondents. The age distribution of the respondents in years ranges from less than or equal to 20 up to 60, as shown in Table I. The sampling adequacy indicator of our survey (KMO) is approximately 0.73 which is greater than the recommended minimum cut-off value of 0.50 (Kaiser, 1974). The Bartlett's test of sphericity is approximately 0.000 which is also less than the recommended maximum cut-off value of 0.050 (Field, 2005). These two statistics justified the use of factor analysis in this paper. The internal consistency of our measurement items (Cronbach's alpha value) is approximately 0.72 which is more than the minimum acceptable cut-off value of 0.60 (Nunnally, 1978). This shows that an acceptable level of reliability has been achieved.

The correlations matrix for the survey item statements and the regression weights are shown in Tables II and III, respectively. It can be seen in the regression weight table that ability and benevolence are more important in terms of users' perception to trust ISPs. Benevolence has a negative impact of −0.282 and 0.395 for ability. On the other hand, integrity weighs just 0.037. The responses from survey respondents indicate a great degree of distrust and unwillingness to take a risk, as demonstrated in the figure immediately below.

The quantitative analysis continues by determining the average percentage response rate for each survey item statement based on the adapted five-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = neutral/neither agree nor disagree; 4 = agree; and 5 = strongly agree). The respondents' support for survey items is shown in Table IV.

We then divide the responses into three distinct categories: positive region of certainty (p-region), region of uncertainty (nu-region) and region of negative certainty (n-region). The *p-region* refers to strongly agree or agree responses while the *nu-region* accounts for uncertain or neutral responses. Finally, the *n-region* represents responses of disagree or strongly disagree. For *p* and *n* regions, we took the average percentage response to provide single values like in the *nu-region*. For instance, the percentage response of the *n-region* for Ability 1 in Figure 4 is calculated as 4.5 + 13.4 = 17.9. The same formula is used for the other survey items in providing a detailed descriptive picture. Figure 5 summarizes the average responses for the survey items.

Our results in Figure 5 indicate that about 52 per cent of respondents trust the competence level of their ISPs. About 42 per cent believe that their ISPs will act appropriately on their behalf. On the contrary, respondents are deeply divided in their opinions in terms of the perception that their ISPs will adhere to acceptable standards, as illustrated in Figure 5. These statistics suggest that Internet users' trust level toward ISPs depends on ability and benevolence more than integrity. This finding contradicts prior result by Mayer *et al.* (1995) who view ability, benevolence and integrity as key trust antecedents. The response rates for survey Questions 3 and 4 (see Section A.3 in Appendix 1) show a great degree of distrust

Table II.
Correlation matrix

	AB1	AB2	AB3	BE1	BE2	BE3	IN1	IN2	IN3	TR1	TR2	TR3
Ability1 (AB1)	1											
Ability2 (AB2)	0.389**	1										
Ability3 (AB3)	0.488**	0.426**	1									
Bene1 (BE1)	0.187**	0.101	0.236**	1								
Bene2 (BE2)	0.350**	0.233**	0.102	0.352**	1							
Bene3 (BE3)	0.312**	0.288**	0.332**	0.446**	0.368**	1						
Integrity1 (IN1)	0.277**	0.112	0.215**	0.419**	0.357**	0.366**	1					
Integrity2 (IN2)	0.296**	0.181*	0.411**	0.342**	0.227**	0.361**	0.195**	1				
Integrity3 (IN3)	0.232**	0.215**	0.498**	0.240**	0.285**	0.263**	0.249**	0.533**	1			
Trust1 (TR1)	0.043	0.008	0.032	−0.114	0.095	−0.114	−0.076	0.075	0.072	1		
Trust2 (TR2)	0.019	−0.003	0.110	−0.020	0.138	0.001	0.003	0.148*	0.119	0.374*	1	
Trust3 (TR3)	0.001	0.135	0.076	−0.037	0.061	−0.064	0.023	0.050	0.053	−0.008	0.081	1

Notes: *Correlation is significant at the 0.05 level (two-tailed); **correlation is significant at the 0.01 level (two-tailed)

	Estimate
Trust ← benevolence	−0.282
Trust ← ability	0.395
Trust ← integrity	0.037
Ability3 ← ability	0.746
Ability2 ← ability	0.584
Ability1 ← ability	0.571
Beneve3 ← benevolence	0.727
Beneve2 ← Benevolence	0.500
Beneve1 ← benevolence	0.642
Integ3 ← integrity	0.787
Integ2 ← integrity	0.679
Integ1 ← integrity	0.295
Trust1 ← trust	0.872
Trust2 ← trust	0.471
Trust3 ← trust	0.025

Table III.
Regression weights

		Responses as percentages				
Survey items	Items statements	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Ability	Ability1	4.5	13.4	28.2	45.5	7.9
	Ability2	7.4	12.4	21.3	39.1	19.3
	Ability3	12.9	18.8	24.8	33.2	9.9
Benevolence	Bene1	23.8	26.7	19.8	20.8	8.4
	Bene2	18.3	17.8	24.3	23.3	13.9
	Bene3	16.8	22.8	16.8	31.7	9.9
Integrity	Integ1	18.3	15.8	33.7	25.2	6.9
	Integ2	15.8	26.2	22.8	23.8	10.9
	Integ3	5.9	23.8	25.2	33.2	10.9
Trust	Trust1	17.3	17.8	16.3	25.2	23.3
	Trust2	17.8	22.3	15.3	35.6	8.9
	Trust3	19.8	13.9	9.9	24.3	32.2

Table IV.
Respondents' support of survey items

and unwillingness on the part of Internet users to take risk with their ISPs, as depicted in Figure 6.

Based on the findings of this study, we propose a revised trust framework depicting key concepts of Internet users' trust level toward ISPs in Kenya, namely, ISPs' ability and benevolence. These two entities are moderated by service deliverability and user protection, as illustrated in Figure 7. The framework also establishes a direct relationship between trust and Internet use.

5. Qualitative results

As we have mentioned earlier, the qualitative results of this study focus on three themes of the interview questionnaire (Appendix 2). The findings in this section also demonstrate a lack of trust between ISPs and users in Kenya. Some of the highlights from interviewees are quoted as follows:

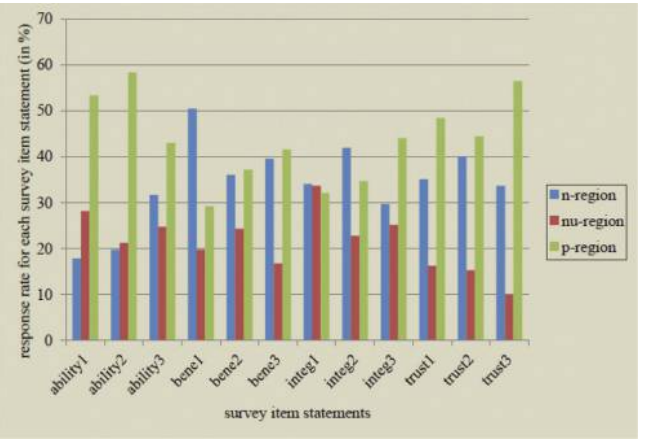

Figure 4.
Average responses for the distinct regions

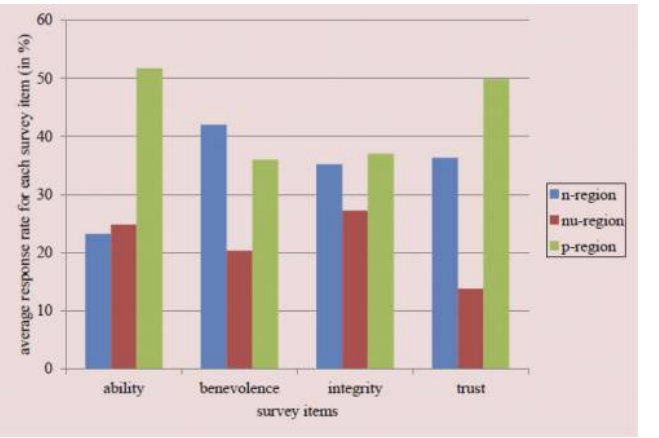

Figure 5.
Average response for survey items

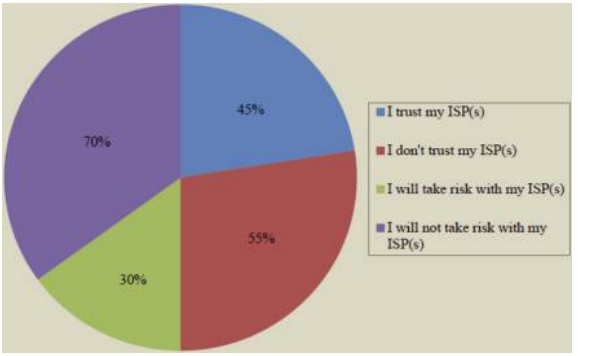

Figure 6.
Respondents' support for trust and risk taking

> The extent of distrust in this country is killing the Internet business and also seriously affecting Internet use. We need to create local forum (for example) as a platform to advocate for the importance of trust in the nation's general ICT dispensation. We cannot afford to ignore this trend (anonymous respondent).

> We are not only experiencing [a]lack of trust between Internet Service Providers and users but among all the major players. There is [a]low level of trust among [ISPs] as well as between [ISPs] and the regulator (anonymous respondent).

> The role of students in trust building is vital in our society in the sense that they can influence the decision of their parents, relatives and peers. This can lead to an improved degree of trust between Internet Service Providers and users in Kenya (anonymous respondent).

> In a normal society, we share the same road [to] a common destination, but in Kenya, we build our own road to a common destination […] This explains the extent of distrust we have in [our] society (anonymous respondent).

> Greed by Internet Service Providers [ISPs] to maximize profit is a major cause of distrust between them and Internet users. However, the [ISPs] will barely acknowledge this phenomenon […] the extent of trust users have for ISPs can potentially increase the use of mobile and electronic applications (anonymous respondent).

The aforementioned interview highlights support our quantitative finding that shows a high degree of distrust between ISPs and users in Kenya. Considering the importance of trust in Internet diffusion, this paper proposes a risk-mitigation framework (Figure 8) that can address distrust and potentially enhance Internet use in a high-risk society. It comprises of four key constructs, namely, trust building, trust violation, trust restoration and implications of trust violation (distrust). The framework is constructed from the four interviews and the 202 responses of our survey questionnaires. It is based on the research participants' opinion on trust building, trust violation, distrust and trust restoration as formulated in our interview themes and Section A.3 of Appendix 1. The framework provides a deeper understanding of how trust can be built and restored once violated. It also accounts for possible causes of trust violation in Kenya's Internet ecosystem and its potential implications (distrust) in Internet diffusion.

It is important to note that creating awareness about potential implications of distrust in Internet dispensation can lead to a wider discussion on trust in societies of high risk. One interview respondent stated the following:

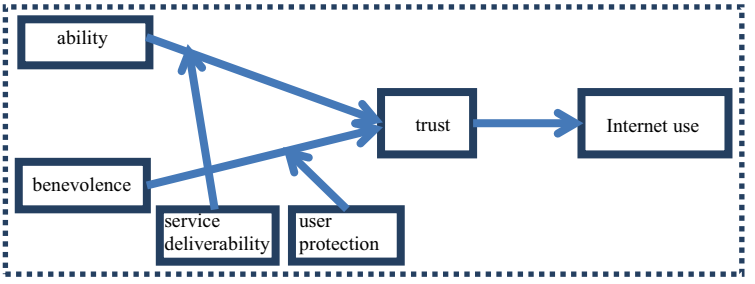

Figure 7.
Revised trust framework

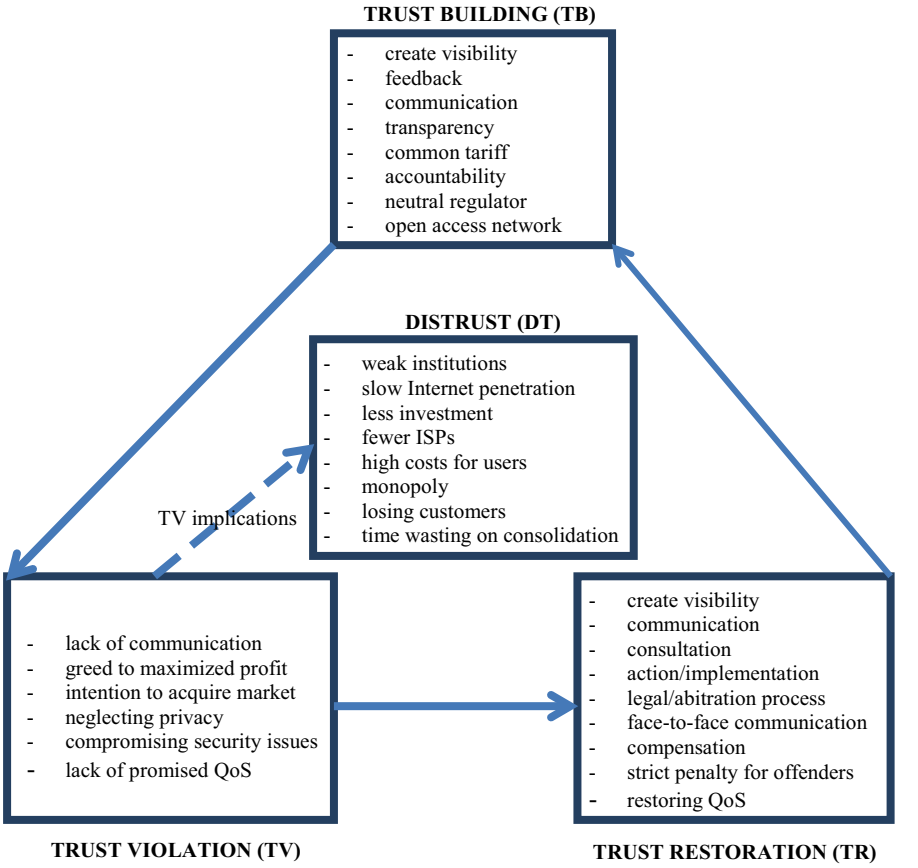

Figure 8.
Risk-mitigation framework

> The significan[ce] of trust can only be appreciated once we are aware of the consequences of distrust […] Trust is one entity that can minimize our perception on issues like privacy and security concerns (anonymous respondent).

It can be seen in Figure 8 that effective communication is an integral part of our proposed risk-mitigation framework. This supports the finding by Savolainen *et al.* (2014) that communication is the key to building and maintaining trust. We suggest computer-mediated communication as a tool that can positively affect and improve communication between Internet users and ISPs. As one interview respondent stated, "improved communication between Internet Service Providers and users can be achieved by using technology-mediated platforms". Respondents also affirmed that computer-mediated communication can be detrimental to trust-building process. As one respondent stated, "people lack trust when they realize that their input […] is not utilized or visible to the public". Respondents highlight that this action can both slow down the trust-building process and cause distrust among people and systems providing mediation platforms. This finding supports previous results that computer-mediated communication increases the risk perception in trust building; indirect interaction

affects the relationship process which can potentially deteriorate or break trust (Hung *et al.*, 2004 and Robert *et al.*, 2009).

6. Discussion

It is important to note that despite various studies on trust, we could not find one that investigates trust between Internet users and ISPs. Therefore, the potential feeling of trust being homogenous in terms of our research context cannot be empirically justified, as we are unable to find prior studies on the theme being investigated. However, there are researchers who take a stance on the idea of trust homogeneity. For instance, Kobayashi *et al.* (2013) enumerate a number of studies within the electronic commerce (EC) context that highlighted the significance of the cultural localization of Web sites. They also cited other prominent researchers like Hoftede (1980 and 1991), Singh (2012) and Singh and Pereira (2005) who underscore the importance of cultural differences in developing effective cross-border EC strategies. According to Kobayashi *et al.* (2013), there are not enough empirical data to claim universal influence of trust for EC and argue that the same trust-building approaches are not applicable across cultures. Consider Africa, for example, as a developing region with a high-risk level (ADB, 2013), one can argue that the trust-building process in this region will surely be different from a developed region. In the trust research, the general theories and measures are likely applicable across cultures, but additional modifications are needed to account for emic constructs and local practices. A cultural view has been suggested as another level of analysis in trust research (Fulmer and Gelfand, 2012).

The aforementioned arguments strengthen the significance of this paper in terms of contributing to knowledge. Furthermore, it addresses the concern highlighted in the study by Joubert and Van Belle (2013) that consumers' ability to trust service providers need to be investigated. Based on the claim by Fulmer and Gelfand (2012) that so far samples of trust research have mainly been Western, this contributes to knowledge by taking into account the context and influence of culture to improve our understanding of trust between Internet users and ISPs from an African perspective. Additionally, the findings of this paper could be replicated in a different context to have a regional comparison of Internet users' trust level toward ISPs. This could serve as another potential contribution to knowledge, as the World Economic Forum report (2011) states that globalization does not lead to homogenization of world cultures. In other words, we cannot assume similarity between developed and developing countries in terms of trust-building process, causes of its violation, potential implications and restoration. In their paper entitled "Conceptualizing initial trust in Internet banking services: a pilot study", Aljaafreh and Al-Ani (2014) state that the lack of trust in developing countries is a major obstacle facing Internet banking adoption compared to developed countries. This argument gives an idea of how the trust process between Internet users and ISPs in Africa might be different from other regions.

This paper has both theoretical and practical implications for researchers, ISPs and ICT policy makers.

From a theoretical perspective, we adapt the Mayer *et al.* (1995) trust model to propose a revised version (Figure 7) that suits an African context. Our proposed framework depicts the key concepts on Internet users' trust level toward ISPs, namely, ISP's ability and benevolence. These two entities are moderated by service deliverability

and user protection, as depicted by Figure 7. The model also establishes a direct relationship between trust and Internet use.

From a practitioner point of view, the proposed risk-mitigation framework (Figure 8) can serve as a vital tool in improving the operational relationship between Internet users and ISPs. It can also help ICT policy makers in Africa to enact policy regulations that will protect Internet users which could eventually improve the level of trust between the continent's Internet users and ISPs. This is possible because the risk-mitigation framework presents how trust can be built, major causes of its violation, its potential implications on wider Internet diffusion and how trust can be restored when violated. Similarly, the proposed revised trust framework can be useful to both ISPs and ICT policy makers in the sense that it highlights specific attributes like service deliverability and user protection that Internet users in Kenya consider as important factors in determining their level of trust toward ISPs. In other words, it possesses both theoretical and practical implications in developing local practices.

In Africa, service deliverability based on service level agreements between Internet users and ISPs barely exists. Even in situations where it does exist, implementation is never a priority except for corporate users like banks, parastatals, embassies, etc. Furthermore, protecting Internet users' interests are non-existing in many African countries. These factors have severe ramifications on trust between Africa's Internet users and ISPs. Our proposed risk-mitigation framework can be used by both ISPs and ICT policy makers to mitigate the aforementioned problems. It can also help improve the operational relationship between Internet users and ISPs. Similarly, our proposed revised trust framework can also serve as a basis for future researchers in developing a more comprehensive trust framework that will capture the typical African context by taking into account cultural and emic issues. It can also help both the research community and practitioners in their effort to enhance Internet diffusion on the continent. This is because the framework includes very relevant and applicable concepts that can potentially enhance Internet adoption in Africa. The importance of trust between Internet users and ISPs cannot be overemphasized. Kyobe (2011b) highlights the capacity to adopt and use technologies as important concepts in determining ICT adoption in South Africa. However, we argue that potential Internet users might not adopt the technology when they lack trust in those providing the services like the ISPs even if Internet users have the capacity to adopt and use the Internet. This signifies the importance of trust in terms of Internet adoption.

7. Conclusion

The key results of this study can be broadly grouped into five themes. They are trust antecedents in Internet use, trust building, trust violation, distrust and trust restoration:

(1) *Trust antecedents*: Mayer *et al.* (1995) suggest three trust antecedents, namely, ability, benevolence and integrity. However, the survey results for this study reveal that Internet users' trust level toward ISPs in Kenya depends more on ISPs' ability in terms of service delivery and their level of benevolence toward Internet users. In other words, ISPs' ability and benevolence in trust building are moderated by service deliverability and user protection. Our respondents' support for integrity as trust antecedent is weaker compared to ability and benevolence. Based on our findings, we propose a revised trust framework (Figure 7) that depicts key concepts from our respondents' perspectives. Both the

survey and interview findings indicate a high degree of distrust in Kenyan society. As one respondent stated, "In a normal society, we share the same road [to] a common destination but in Kenya, we build our own road to a common destination […]". In other words, things are done differently in Kenya in that making their own boundaries means a lesser degree of trust.

(2) *Trust building*: Based on the findings of a great degree of distrust between ISPs and user in Kenya, this study underlines a number of things that can enhance trust building in this high-risk environment. Trust building and enhancement are related to two main themes. The first one concerns relationship interaction including feedback, communication and visibility. The second one refers to ethical and contract issues in service delivery, including transparency, common tariff, accountability, neutral regulation and an open access network.

(3) *Trust violation*: A number of factors can undermine Internet users' perception of ISPs' ability to be trusted. This paper found several factors, namely, a lack of communication, greed for maximized profit, intention to acquire the market, neglecting privacy, compromising security and a lack of promised quality of service (QoS).

(4) *Distrust*: This is one negative ramification of trust violation which can impede Internet use in a number of ways. These can include weak institutions, slow Internet penetration, less investment, fewer ISPs, high costs for users, monopolization, lose customers and considerable time wasted on consolidation.

(5) *Trust restoration*: It is possible to restore trust once violated that ISPs should take into account. This paper provides a number of ways through which trust restoration could be achieved such as creating visibility, improved communication, consultation, action/implementation, a legal/arbitrary process, face-to-face communication, compensation, strict penalties for offenders and restoring QoS.

Another key finding of this study is by conceptualizing trust building, trust violation, distrust and trust restoration into a risk mitigation (Figure 8). In conclusion, the two proposed frameworks herein could enhance our understanding of trust in Internet diffusion and potentially increase use in Kenya and other high-risk countries. This is because the framework can be used to sensitize ISPs to improve their operational relationship with their respective Internet users. They can also serve as guiding tools for ICT policy makers and ISPs in high-risk societies like Africa in terms of their operational relationship with Internet users.

There are several limitations of this study. First, most of the data were collected from students at a single university. Second, the authors used a 0.10 precision value instead of 0.05 in determining their sample size of the target population. This provides a weaker argument in terms of generalizing the results. Third, a limited number of ISPs participated in the research. The survey could have had more ISPs participating in the study to capture a broader perspective. Fourth, respondents in Kenya are very sensitive to issues relating to the role of government in Internet diffusion. This has to do with their individual perception that any negative statement they say about government is tantamount to sabotage and could warrant prosecution; this situation is completely different in developed countries. These particular attributes of fear and reservation were

evident during the data collection. It is fair to acknowledge that some responses might not reflect the true perception of the respondents but instead influenced by the sensitivity to discuss the role of government. Finally, another difficulty in collecting data in Kenya relates to the lack of awareness about the importance of research. A CEO of a renowned Internet ISP stated the following:

> I have to tell you the fact […] we don't see the importance of collecting data from us in order to help improve Internet use in Kenya. This is just a waste of time and we are not obliged to participate […] I am sorry but that is the reality.

Notwithstanding, it must be noted that the aforementioned limitations are, however, beyond the authors' control, given the nature of the research context and associated difficulty in collecting data in an African country compared to Europe or America. Future research should focus more on contextual qualitative studies on cultural and local practices of the role of trust and its development in high-risk contexts. It is also imperative to apply our proposed frameworks to come up with more comprehensive trust and risk-mitigation frameworks that will depict emic constructs and local practices in an African context.

References

African Development Bank (ADB) (2013), "Final report on needs assessment for risk mitigation in Africa: demands and solutions", Initiative for Risk Management in Africa (IRMA).

Air University Sampling and Surveying Handbook (2002), "Guidelines for planning, organizing and conducting surveys, revised (PDF) edition", available at: www.au.af.mil/au/awc/awcgate/edref/smpl-srv.pdf (accessed 22 July 2014).

Aljaafreh, A. and Al-Ani, A. (2014), "Conceptualizing initial trust in Internet banking services: a pilot study", in Strahonja, V., Vrcek, N., Plantak, D., Vukovac, P., Barry, C., Lang, M., Linger, H. and Schneider, C. (Eds), *Information Systems Development: Transforming Organizations and Society Through Information Systems (ISD2014 Proceedings)*, *Varaždin*.

Alshameri, F. and Banjura, A.K. (2014), "Creating a metadata to study and teach about African issues", *Information Technology & People*, Vol. 27 No. 3, pp. 341-365.

Audi, R. and Murphy, P.E. (2006), "The many faces of integrity", *Business Ethics Quarterly*, Vol. 16 No. 1, pp. 3-21.

Avgerou, C. (2008), "Information systems in developing countries: a critical research review", *Journal of Information Technology*, Vol. 23 No. 3, pp. 133-146.

Bankole, F.O., Bankole, O.O. and Brown, I. (2011), "Mobile banking adoption in Nigeria", *The Electronic Journal of Information Systems in Developing Countries*, Vol. 47 No. 2, pp. 1-23.

Blanchard, A.L., Welbourne, J.L. and Boughton, M.D. (2011), "A model of online trust", *Information, Communication & Society*, Vol. 14 No. 1, pp. 76-106.

Burke, C.S., Sim, D.E., Lazzara, E.H. and Salas, E. (2007), "Trust in leadership: a multi-level review and integration", *The Leadership Quarterly*, Vol. 18 No. 6, pp. 606-632.

Casielles, R.V., Alvarez, L.S. and Martin, A.M.D. (2005), "Trust as a key factor in successful relationships between consumers and retail service providers", *Service Industry Journal*, Vol. 25 No. 1, pp. 83-101.

Cho, D-Y., Kwon, H.J. and Lee, H-Y. (2007), "Analysis of trust in Internet and mobilecommerce adoption", *Proceedings of the 40th Hawaii International Conference on System Sciences*, *Waikoloa, HI*.

Connell, J., Ferres, N. and Travaglione, T. (2003), "Endengering trust in manager subordinate relationships: predictions and outcomes", *Personal Review*, Vol. 32 No. 5, pp. 569-587.

Costa, A.C. (2003), "Measuring trust in teams: development and validation of the trust team inventory", *Australian Journal of Psychology*, Vol. 55, p. 120.

Dalberg Survey Report (2013), "Impact of the Internet in Africa: establishing conditions for success and catalyzing inclusive growth in Ghana, Kenya, Nigeria and Senegal", available at: www.impactoftheinternet.com (accessed 22 July 2014).

Das, T.K. and Teng, B.S. (2001), "Trust, control and risk in strategic alliances: an integrated framework", *Organizational Studies*, Vol. 22 No. 2, pp. 251-283.

Davis, G.M. (1999), "A test of an interpersonal trust model (integrity, benevolence)", PhD Dissertation, University Microfilms International, Ann Arbor, MI.

Davis, J.H., Schoorman, F.D., Mayer, R.C. and Tan, H.H. (2000), "The trusted general manager and business unit performance: empirical evidence of competitive", *Strategy Management Journal*, Vol. 21 No. 5, pp. 563-576.

Eriksson, P. and Kovalainen, A. (2008), *Qualitative Methods in Business Research*, SAGE, London.

Field, A.P. (2005), *Discovering Statistics Using SPSS*, 2nd ed., Sage, London.

Fukuyama, F. (1995), *Trust: The Social Virtues and Creation of Prosperity*, Free Press, New York, NY.

Fulmer, C.A. and Gelfand, M.J. (2012), "At what level (and in whom) we trust: trust across multiple organizational levels", *Journal of Management*, Vol. 38 No. 4, pp. 1167-1230.

Gill, H., Boes, K., Finegan, J. and McNally, J. (2005), "Antecedents of trust: establishing a boundary condition for the relationship between propensity to trust and intention to trust", *Journal of Business & Psychology*, Vol. 19 No. 3, pp. 287-302.

Glasow, P.A. (2005), "Fundamentals of survey research methodology", MITRE, Washington, available at: www.mitre.org/work/tech_papers/tech_paper/tech_paper_05/05_0638/05_0638.pdf (accessed 22 July 2014).

Grabner-Krauter, S. and Kalushaha, E.A. (2003), "Empirical research in online trust: a review and critical assessment", *International Journal of Human-Computer Studies*, Vol. 58 No. 1, pp. 783-812.

Green, J.C. (2007), *Mixed Methods in Social Inquiry*, Jossey-Bass, San Francisco, CA.

Hung, Y.T.C., Dennis, A.R. and Robert, L. (2004), "Trust in virtual teams: towards an integrative model of trust formation", *Proceedings of the 37th Hawaii International Conference on System Science, Big Island, HI*, pp. 1-11.

International Telecommunication Union (ITU) (2013), "ICT facts and figures", available at: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013e.pdf (accessed 22 July 2014).

International Telecommunication Union (ITU) (2014), "ITU world telecommunication/ICT indicators database", available at: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf (accessed 22 July 2014).

Hofstede, G. (1980), *Culture's Consequences: International Differences in Work-Related Values*, Sage, Beverely Hills, CA.

Hofstede, G. (1991), *Cultures and Organizations: Software of the Mind*, McGraw-Hill, London.

Johnson, B.B. (2003), "Are some risk comparison more effective under conflict? A replication and extension of Roth *et al*", *Risk Analysis*, Vol. 23 No. 4, pp. 767-780.

Joubert, J. and Van Belle, J-P. (2013), "The role of trust and risk in mobile commerce adoption within South Africa", *International Journal of Business, Humanities and Technology*, Vol. 3 No. 2, pp. 1-12.

Kaiser, H.F. (1974), "An index of factorial simplicity", *Psychometrika*, Vol. 39, pp. 31-36.

Kerlinger, F.N. (1986), *Foundation of Behavioral Research*, Holt, Rinehart and Winston, New York, NY.

Kobayashi, T., Okada, H., Cooharojananone, N., Bracamonte, V. and Suzuki, T. (2013), "How can electronic commerce in developing countries attract users from developed countries? A comparative study of Thailand and Japan", *International Journal of Electronic Commerce Studies*, Vol. 4 No. 2, pp. 159-184.

Koehn, D. (2005), "Integrity as a business asset", *Journal of Business Ethics*, Vol. 58 Nos 1/3, pp. 125-136.

Kuriyan, R., Kitner, K. and Watkins, J. (2010), "ICTs, development and trust: an overview", *Information Technology & People*, Vol. 23 No. 3, pp. 216-221.

Kyobe, M. (2011a), "Special issue on information and communication technology in South Africa", *Journal of Systems and Information Technology*, Vol. 13 No. 3, pp. 255-267.

Kyobe, M. (2011b), "Investigating the key factors influencing ICT adoption in South Africa", *Journal of Systems and Information Technology*, Vol. 13 No. 3, pp. 255-267.

Leahy, K.B. and Yermis, I.V. (2003), "Information and communication technology: gender issues in developing nations", *Informing Science Journal*, Vol. 6, pp. 143-155.

Linder, A. and Santiso, C. (2003), "Not everything that counts can be counted: a critical look at risk ratings and governance indicators", *Nordic Journal of Political Economy*, Vol. 29, pp. 105-132.

McEvily, B., Perrone, V. and Zaheer, A. (2003), "Trust as an organizing principle", *Organizational Science*, Vol. 14 No. 1, pp. 91-103.

McKnight, D.H., Cummings, L.L. and Chervany, N.L. (1998), "Initial trust formation in new organizational relationships", *Academy of Management Review*, Vol. 23 No. 3, pp. 473-490.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995), "An integrative model of organization trust", *Academy of Management Review*, Vol. 20 No. 3, pp. 709-734.

Miles, M.B. and Huberman, A.M. (1987), *Qualitative Data Analysis: A Sourcebook for New Methods*, 5th ed., SAGE Publications, Beverly Hills, CA, London, New Delhi.

Mofleh, S., Wanous, M. and Strachan, P. (2008), "Developing countries and ICT initiatives: lessons learnt from Jordan's experience", *The Electronic Journal Information of Systems Evaluation*, Vol. 34 No. 5, pp. 1-17.

Nunnally, J. (1978), *Psychometric Theory*, McGraw Hill, New York, NY.

Pinsonneault, A. and Kraemer, K.L. (1993), "Survey research methodology in management information systems: an assessment", *Journal of Management Information Systems*, Vol. 10 No. 2, pp. 75-105.

Popola, N.F. (2013), "The effect of trust in adoption of internet banking: a case study of Nigeria", *International Journal of Economic and Business Management*, Vol. 1 No. 2, pp. 19-24.

Raji, M.O., Ayoade, O.B. and Usoro, A. (2006), "The prospects and problems of adopting ICT for poverty eradication in Nigeria", *The Electronic Journal on Information Systems in Developing Countries*, Vol. 28 No. 8, pp. 1-9.

Rath, L.E. (1972), *Meeting the Needs of Children: Creating Trust and Security*, Merrill, Columbus, OH.

Robert, L.P., Denis, A.R. and Hung, Y.-T.C. (2009), "Individual swift trust and knowledge-based trust in face-to-face and virtual team members", *Journal of Management Information Systems*, Vol. 26 No. 2, pp. 241-279.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. (1998), "Not so different after all: across-disciplinary view of trust", *Academy of Management Review*, Vol. 23 No. 3, pp. 393-404.

Sahey, S. and Avgerou, C. (2002), "Introducing the special issue on information and communication technologies in developing countries", *The Information Society*, Vol. 18, pp. 73-76.

Salgado, S. (2012), "The web in African countries", *Information, Communication & Society*, Vol. 15 No. 9, pp. 1373-1389.

Savolainen, T. and Häkkinen, S. (2011), "Trusted to lead: trustworthiness and its impact on leadership", *Technology Innovation Management Review*, pp. 52-56, available at: http://timreview.ca/article/429

Savolainen, T. and Lopez-Fresno, P. (2013), "Trust as intangible asset- enabling intellectual capital development by leadership for vitality and innovativeness", *The Electronic Journal of Knowledge Management*, Vol. 11 No. 2, pp. 244-255.

Savolainen, T., Lopez-Fresno, P. and Ikonen, M. (2014), "Trust-communication dyad in inter-personal workplace relationships – dynamics of trust deterioration and breach", *The Electronic Journal of Management*, Vol. 12 No. 4, pp. 232-240.

Serva, M.A., Fuller, M.A. and Mayer, R.C. (2005), "The reciprocal nature of trust: a longitudinal study of interacting teams", *Journal of Organizational Behavior*, Vol. 26 No. 6, pp. 625-648.

Singh, N. (2012), *Localization Strategies for Global e-Commerce*, Cambridge University Press, Cambridge.

Singh, N. and Pereira, A. (2005), *The Culturally Customized Web Site*, Elsevier Butterworth-Heinemann, Burlington, MA.

Six, F. (2005), *The Trouble with Trust: The Dynamics of Interpersonal Trust Building*, Edward Elgar Publishing, Cheltenham.

Strauss, A.L. (1987), *Qualitative Analysis for Social Scientists*, Cambridge University Press, New York, NY.

Thaw, Y.Y., Mahmood, A.K. and Dominic, P.D.D. (2009), "A study on factors that influence the consumers' trust on e-commerce adoption", *International Journal of Computer Science and Information Security*, Vol. 4 Nos 1/2, pp. 1-7.

Walsham, G. and Sahey, S. (2006), "Research on information systems in developing countries: current landscape and future prospects", *Information Technology for Development*, Vol. 12 No. 1, pp. 7-24.

Williams, M. (2001), "In whom we trust: group membership as an affective context for trust development", *Academy of Management Review*, Vol. 26 No. 3, pp. 377-396.

World Economic Forum (WEF) (2011), "The new Internet world: a global perspective on freedom of expression, privacy, trust and security online", A Contribution to the Global Information Technology Report 2010-2011 Transaction 2.0, WEF.

Xu, R. and Ba, S. (2005), "Analysis of online trust building technologies", *Seminar Paper Contemporary Issues on e-Commerce, University of Manheim, Department of Information Systems*.

Zeffane, R. (2010), "Towards a two-factor theory of interpersonal trust: a focus on trust in leadership", *International Journal of Commerce and Management*, Vol. 20 No. 3, pp. 246-257.

Further reading

Bentler, P.M. and Bonett, D.G. (1980), "Significance tests and goodness of fit in the analysis of covariance structures", *Psychological Bulletin*, Vol. 88 No. 3, pp. 588-606.

Brown, M.W. and Cudeck, R. (1993), "Alternative ways of assessing model fit", in Bollen, K.A. and Long, J.S. (Eds), *Testing Structural Equation Models*, Sage Publications, Newbury Park, CA, pp. 136-162.

Butler, J.K. Jr (1991), "Toward understanding and measuring conditions of trust: evolution of conditions of trust inventory", *Management Journal*, Vol. 17 No. 3, pp. 643-663.

Carter, R.L. (2006), "Solutions for missing data in structural equation modeling", *Research & Practice in Assessment*, Vol. 1 No. 1, pp. 1-6.

Conchie, S.M., Taylor, P.J. and Charlton, A. (2011), "Trust and distrust in safety relationship: mirror reflection", *Safety Science*, Vol. 49 Nos 8/9, pp. 1208-1214.

Csik, M. (2012), "Trust breach and restoring of violated trust: a narrative study of the stories from finnish workplaces", A Master's thesis, Department of Business Studies, Faculty of Social Sciences and Business Studies, University of Eastern Finland, Joensuu.

Cummings, L.L. and Bromiley, P. (1996), "The organizational trust inventory (OTI)", in Kramer, R.M. and Tylor, T.R. (Eds), *Trust in Organizations: Frontiers of Theory and Research*, Sage, Thousand Oaks, CA, pp. 302-330.

Hoe, S.L. (2008), "Issues and procedures in adopting structural equation modeling technique", *Journal of Applied Quantitative Methods*, Vol. 3 No. 1, pp. 76-83.

Hooper, D., Coughlan, J. and Mullen, M.R. (2008), "Structural equation modeling: guideline for determining model fit", *The Electronic Journal of Business Research Methods*, Vol. 6 No. 1, pp. 53-60.

Hossain, L. and Wigand, R.T. (2004), "ICT enabled virtual collaboration through trust", *Journal of Computer-Mediated Communication*, Vol. 10 No. 1.

Johnston, A.C. and Warkentin, M. (2002), "The online consumer trust construct: a web merchant practitioner perspective", *Proceedings of the Seventh Annual Conference, South Association for Information Systems, Savannah, GA*, pp. 221-226.

Langmia, K. (2005), "The role of ICT in economic development of Africa: the case of South Africa", *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, Vol. 2 No. 4, pp. 144-156.

Mayer, R.C. and Davis, J.H. (1999), "The effect of the performance appraisal system on trust for management: a field quasi-experiment", *Journal of Applied Psychology*, Vol. 84 No. 1, pp. 123-136.

Möllering, G. (2005), "The trust/control duality-an integrative perspective on positive expectations of others", *International Sociology*, Vol. 20 No. 3, pp. 283-305.

Robert, J.R., Dennis, A.R. and Hung, Y.T.C. (2009), "Individual swift trust and knowledge-based trust in face-to-face and virtual team members", *Journal of Management Information Systems*, Vol. 26 No. 2, pp. 241-279.

Tan, H.H. and Tan, C.S. (2000), "Toward the differentiation of trust in supervisor and trust in organization", *Genetic, Social & General Psychology Monographs*, Vol. 12 No. 2, pp. 241-261.

United States Central Intelligence Agency (CIA) (2012), available at: www.cia.gov (accessed 22 July 2014).

Weston, R. and Gore, P.A. Jr (2006), "A brief guide to structural equation modeling", *The Counseling Psychologist*, Vol. 34 No. 5, pp. 719-751.

World Internet Statistics (2012), "World internet statistics", available at: www.internetworldstats.com (accessed 22 July 2014).

Appendix 1. Survey

Survey questionnaire

Section A.1: Demographic information (*Please select as appropriate*)

The objective of the demographic information is essentially meant to provide us with a deeper understanding of factors such as gender, income, occupation and place of Internet access in Internet adoption phase in Sub-Saharan Africa.

1. gender: female [ ] male [ ]
2. age: [≤ 20] [21 – 25] [26 – 30] [31 – 35] [36 – 40] [41 – 45] [46 – 50] [51 – 55] [56 – 60] [≥ 61]

Section A.2: Trust antecedent (*Please select as appropriate*)

This section is meant to determine the key trust antecedents that influence Internet users' perception toward Internet Service Provider(s).

survey item	item statement	five point Likert-scale (1=strongly disagree; 2=disagree; 3=neither agree nor disagree; 4=agree; 5=strongly agree)				
		1	2	3	4	5
ability	My Internet Service Provider is very capable of performing its function.					
	My Internet Service Provider appears to be successful at the services they offer.					
	I feel very comfortable about my Internet Service Provider's skills.					
benevolence	My Internet Service Provider is concerned about my welfare.					
	My needs and desires are very important to my Internet Service Provider.					
	My Internet Service Provider really looks out for what is important to me.					
integrity	My Internet Service Provider has a strong sense of justice.					
	I will never have to wonder whether my Internet Service Provider will stick to his/her word in terms of service delivery and my security.					
	My Internet Service Provider's actions and behaviors are not very consistent.					
trust	If I had my way, I wouldn't let my Internet Service Provider have any influence over issues that are important to me.					
	In dealing with my Internet Service Provider, I am cautious until they have provided proof that they are trustworthy.					
	I am cautious about my Internet Service Provider or else they could take advantage of me.					

Section A.3: Risk mitigation framework (*Please answer this section as candidly as possible*)

This section has two objectives. The first is to find out whether Internet users in Nairobi trust their Internet Service Providers (ISPs). The second one is to determine how to build trust between ISPs and users, common causes of trust violation, implications of distrust and how to restore trust.

3. As an Internet user, I trust my Internet Service Provider(s).
   yes [ ] no [ ]
4. I don't trust my Internet Service Provider(s).
   yes [ ] no [ ]
5. I am willing to take risks in dealing with my Internet Service Provider(s).
   yes [ ] no [ ]

(*continued*)

6. I am not willing to take risks in dealing with my Internet Service Provider(s).

yes [ ] no [ ]

7. Please specify how to develop trust between Internet Service Providers and users.

8. What are the major causes of trust violation between you and your ISP(s)?

9. What are the potential implications of distrust (trust violation)?

10. What major steps can be taken to restore trust when violated?

Appendix 2. Interview

Interview questionnaire:

(1) The role of trust:
- What is the role of leadership in generating ICT policies?
- What is the role of trust in this process?
- How do you perceive the role of trust in generating ICT policies to enhance Internet use?
- Who are the main actors in the network of Internet diffusion in Kenya?

(2) What is trust, how it is perceived and manifested:
- What is the trust level between Internet service providers/regulators and users?
- How do you perceive trust in the network of regulators/providers/users?
- How is trust manifested in your work and network contexts?
- How do you build trust in your efforts to provide Internet access to users?

(3) e-Trust and e-Leadership:
- What is your perception *of* e-context and technology mediation in leadership?
- Does e-context and technology mediation in leadership build/deteriorate trust? If so, how?
- Does e-context and technology mediation enhance trust building?

(4) Trust and (in) Internet diffusion*:
- What is the role of trust in Internet diffusion?**
- How do you see the role and existence of trust among leaders, Internet service providers and users in Kenya?
- How do you build trust in the context of Internet diffusion in Kenya?**
- What is the role of distrust in this process?**
- Does distrust exist among network actors involved in terms of Internet diffusion in Kenya?

(5) Trust building and maintenance*:
- How is trust initiated and built in relationships between a leader and a follower?
- How is trust maintained between leaders, Internet service providers and users in Kenya?
- What are the main factors that build trust in Internet diffusion in Kenya?**

(6) Distrust, trust breach and restoring trust*:
- Have you experienced distrust? If so what causes distrust?
- What are the main factors that cause distrust in Internet diffusion in Kenya?**
- What are the main factors that violate trust in Internet diffusion in Kenya?**
- What leads to breach of trust?**
- How can trust be restored if violated or broken?** (*= Themes that are utilized in this paper; ** = Questions that are utilized in this paper)

About the authors

Almamy Touray is a PhD candidate at the Department of Computer Science and Information Systems at the University of Jyväskylä in Finland. He obtained a Master's degree in Computational Engineering and a Bachelor of Science degree (Honors) in Computer Science. His research interests include ICT for development, Internet adoption and diffusion. Almamy Touray is the corresponding author and can be contacted at: almamy.2.touray@jyu.fi

Taina Savolainen is a Professor of Management and Leadership at the University of Eastern Finland's Business School. She leads the Research Group of Trust within organizations focusing on trust development in intra-organizational work relationships. She is specializing in process studies of trust within organizations, and is also an expert in leadership, organizational change and global competitiveness management. She is an internationally recognized scholar in leadership and trust education with a large number of international academic publications and writings for professional practice. Her academic achievements have been recognized in Who's Who in the World.

Airi Salminen is a Professor Emerita of Digital Media in the Department of Computer Science and Information Systems at the University of Jyväskylä in Finland. She has been the head of several research projects where research has been tied to ICT development efforts in major Finnish companies and public sector organizations. Long-term research collaboration with the Finnish Parliament and Government has produced a great number of research articles and practical results in the information management environment of the Parliament and Government. She has worked for three periods at Canadian universities: first as a Visiting Research Associate at the University of Western Ontario and later as a Visiting Professor at the Universities of Waterloo and Toronto. Her current research interests include ICT for development, enterprise content management, structured documents and e-government.

Erkki Sutinen is a full professor of Computer Science at the University of Eastern Finland. His research interests include the uses of information and communication technologies for

development (ICT4D), computer science and ICT education, creative problem solving, contextual design and text tools for learning. He has been designing innovative educational approaches in developing countries and for special education. He has a six million euros portfolio of research and development projects funded by various EU sources, Academy of Finland and the Finnish Funding Agency for Technology and Innovation (TEKES). He has been working as a visiting assistant professor at Purdue University, an associate professor at University of Linköping in Sweden, a visiting professor at University of Pretoria, an adjunct professor at Tumaini University in Tanzania and an honorary research fellow at Massey University in New Zealand. In 2010-12, he was an extraordinary professor at North-West University in South Africa.

Yue Dai is a researcher at the edTech research group, School of Computing, University of Eastern Finland. She received her PhD in computer science from the University of Eastern Finland in 2013. Her main research interests are strategy management, competitive intelligence, text mining and sentiment analysis.