African Journal of Business Management Vol. 5(14), pp. 5524-5535,18 July, 2011
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM11.682
ISSN 1993-8233 ©2011 Academic Journals

Full Length Research Paper

Trust and security of electronic banking services in Saudi commercial banks: Saudis versus Non Saudis opinions

Mohamed Osman Shereif Mahdi

Department of Management and Marketing, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.
E-mail: mosmahdi@kfupm.edu.sa. Tel: +966-3-8607268. Fax: +966-3-8602544.

Accepted 20 April, 2011

This paper reports on research conducted in the Kingdom of Saudi Arabia. The research examines the trust and the security of electronic banking services in Saudi commercial banks. The design for the study used quantitative research methodology. Data were collected by means of questionnaires utilizing snowballing approach. 500 Questionnaires were distributed to banks' respondents including Saudi and Non Saudi banks' customers. The quantitative data presented very strong evidence to support both hypotheses that: *there are significant trust differences between Saudis and Non Saudis in their use of electronic banking services comprising ATM, Credit cards, Mobile SMS, Phone and the Internet banking (p-value* 0.001, 0.006, 0.004, 0.000 and 0.033 respectively*)*; and also that: *there are significant security differences between Saudis and Non Saudis in their use of electronic banking services including ATM, mobile SMS, phone and the internet banking services (p-value 0.000, 0.000, 0.000* and *0.006, respectively).* Findings revealed how Saudi banks' customers have very high trust in using the electronic banking services and also how Saudi banks' customers strongly believed that the electronic banking services are more secure compared with their counterpart the Non Saudis. The study presents new empirical evidence, and enhances our understanding on the trust and the security of electronic banking technology in a Middle East country. The implication of this study will be vital in helping Saudi banks' managers to assess and identify methods of improving the trust and the security of electronic banking services offered.

Key words: Electronic security, information technology, e-services trust, technological change, electronic banking, developing countries, Middle East, Saudi Arabia.

INTRODUCTION

This study reports on research that was conducted in the Kingdom of Saudi Arabia (KSA) to examine the trust and the security of electronic banking services in Saudi banks. Saudi Arabia is the world's largest producer and exporter of total petroleum liquids, and the world's second largest crude oil producer. The KSA holds more than 20% of the world's proven oil reserves, and plays a leading role in OPEC. Saudi Arabia's economy remains heavily dependent on oil and petroleum-related Industries, including petrochemicals and petroleum refining (EIA, 2011). Initial investigation reveals insufficiency of research in the field of management of information technology (IT) and change in developing countries and that there is little information about trust and security of electronic banking services in Saudi commercial banks. In general, banks operate in an information system context whereby financial institutions are critically dependent on information technology activity for their daily operations. However, selecting one industry sector such as Saudi banking industry, rather than different industries, offers some advantages to research since respondents in the same industry are working in similar surroundings and are more likely to have similar skills and backgrounds that may promote homogeneity of data. Saudi banking industry in the Eastern Province has been identified as an industry that plays a crucial role in the economic development of the Kingdom of Saudi Arabia as well as providing valuable electronic banking

services to both indigenous people and huge number of expatriates residing and working in the Eastern Province of the Kingdom.

This study focuses on investigating and presenting findings on trust and security of electronic banking services in Saudi banking sector. The research compares Saudi banks customers' opinions with their counterpart the Non Saudis on trust and security of electronic banking services in the commercial banking sector of Saudi Arabia in the Eastern Province. The implication of this study will be critical in helping Saudi banking practitioners to assess and identify methods of improving trust and security of electronic banking services in Saudi banking industry. The study begins with research objectives, briefly examines literature on IT, security and trust, followed by research methodology, then presents findings and discussion and closing with conclusion.

Research objectives

The paper objectives were set to examine trust and security of electronic banking services in Saudi commercial banks. The study aims at assessing both the degree of trust and security among banks' customers on the electronic banking services comprising ATMs, credit cards, telephone banking, mobile SMS, and Internet banking services in the Easter Province of the Kingdom including Dhahran, Khobar, Dammam and Jubail.

The design for the study used research methodology which included quantitative technique. Data were collected by means of distributing questionnaires to bank respondents including both Saudi and Non Saudi banks' customers through snowballing approach. Statistical Package for Social Scientists (SPSS) for Windows package was employed for the analysis of the data collected from the survey. The method of analysis consisted of descriptive statistics including mean, variance and frequencies. The researcher used independent-samples t-test to test for statistical significance of the research hypotheses.

In completion, it is hoped that the study enhances the understanding of academicians, professional managers and banking practitioners alike of the trust and the security of electronic banking services in a banking sector of a developing country such as Saudi Arabia.

LITERATURE REVIEW

The literature review examines studies on information technology (IT) and change in the banking industry including trust and security of electronic banking services. In the last decade, computer-based information technology (IT) had become essential in most organizations, and had a major influence on the development of electronic services in the banking industry all over the world. The increase use and rapid developments of information technology enabled fundamental changes in how companies including banks interact with customers (Dabholkar and Bagozzi, 2002; Parasuraman and Zinkhan, 2002, Bauer et al., 2005). Whether banking organizations are newly established or fully mature, they maintain their vitality by innovating, changing, and learning from their experiences (Hellriegel, et al., 2005; Slocum, et al., 2008). Although information technology has attracted a number of academic researchers and banking practitioners alike (Zeithaml, 2002; Zeithaml et al., 2002; Zhang and Prybutok, 2005; Lee and Lin, 2005; Bauer et al., 2005), there is still a considerable gap of knowledge on the issue of electronic banking services and the wider issue of technological change in the banking industry of developing countries (Parasuraman and Zinkhan, 2002). This relative lack of knowledge is particularly a problem to companies seeking to meet customer expectations and requirements by offering consistently high, favourably perceived service standards of electronic banking services in a rapidly changing technological environment. As such, employment of IT is a major challenge facing business organizations seeking to sustain competitive advantage in dynamic business markets including commercial banking sector. This challenge is more complex in developing countries particularly in the Middle East where business organizations deal with problems such as inadequate investment, and lack of involvement in the management process of new technology and change (Mahdi and Dawson, 2007).

The history of technology in banking highlights how IT has changed the methods by which the banking sector operate, for instance, 50 per cent of foreign exchange business trades are carried out through IT (Childs, 1994). International banks as Harris (2001) points out are considered to be large investors in technology. Moreover, worldwide banks have invested heavily, for example, in telecommunications networks and SWIFT to link overseas branches with their headquarters in order to enable banks to effectively communicate business across the globe regardless of time and distance (Dixon, 2002; Marlin, 2004). As the banking external environments become increasingly competitive and turbulent, the most effective organizations would be those that build change, innovation, and learning into their normal operations (Hellriegel et al., 2005; Slocum et al., 2008). However, the issue is no longer a question of whether IT is used or not, rather the issue is how best it is efficiently used for sustainable and competitive advantage. The vast majority of people who uses banking technology such as ATM and or the Internet, for instance, can fully understand this. Moreover, the improvements in the trust and the security of electronic services are not merely appreciated by customers, but have become very important to effectively utilization of information banking technology.

Prior to the development of a conceptual framework for this study , it is important to define electronic banking

services. The current literature lacks a comprehensive definition of electronic and or automated service. Electronic banking in its simplest form may mean the provision of information about the bank and its products by means of a page on the Internet. Daniel (1999) defines the term as 'the provision of information and or services by a bank to its customers via computer, telephone or television'. A more developed service, in Daniel's (1999) view, is one that provides the customers with the opportunity to gain access to their accounts, carry out transactions or buy products online or using other electronic means such as TV, telephone or automated teller machines (ATMs). This research, draws on Daniel's (1999), as it provides a more general definition of automated banking services that can be extended beyond ATMs, telephone and Internet banking as they are not the only automated services in the banking industry. This study would suggest that electronic banking services include ATMs, SWIFT, credit cards, telephone banking, mobile SMS, interbranch online, and Internet banking services.

Therefore, the study defines electronic banking services as 'the provision of information and or services by a bank to its customers through ATMs, SWIFT, credit cards, telephone banking, mobile SMS, interbranch online, and or Internet banking services'.

CONCEPTUAL FRAMEWORK

In developing a framework to study trust and security of electronic banking services in Saudi banks, the initial literature review reveals a number of models which can fit with this study including Technology Acceptance Model (TAM), was developed from Theory of Reasoned Action (TRA) by Davis (1989); Technology Acceptance Model (TAM2) was developed by Venkatesh and Davis (2000); the Unified Theory of Acceptance and Use of Technology (UTAUT) was introduced by Venkatesh et al. 2003) with four core determinants of intention and usage, and up to four moderators of key relationships. The UTAUT was formulated by theorising four constructs to play an important role as direct determinants of user acceptance and usage behaviour (Kripanont, 2007). The extended TAM was further developed by Al-Sukkar (2005), and further developed by Al-Somali et al. (2009) with four core dependent variables of intention and usage comprising: *Perceived Usefulness, Perceived Ease of Use, Attitude Towards Use, Actual Usage*, and number of independent control variable including *Quality of electronic services, Age, Gender, Education, Income, Trust, and Culture* (Al-Sukkar, 2005; Al-Somali et al., 2009). However, Al-Sukkar (2005) and Al-Somali et al. (2009) research in Jordon and the Kingdom of Saudi Arabia respectively, could be considered as more fitting with this study, and that there are a number of elements that the researcher can draw upon from these models. In studying trust and security of electronic banking services the demographics such as *age, gender, education, and income* are also taken into consideration and included into the framework as briefly discussed as follows:

1. Demographics: are the characteristics of a work group, an organization, a specific market, or various populations, such as age, gender, education, occupation, and income. Demographics play an important role in marketing, advertising, and human resources management (Slocum, et al., 2008). The review of the literature reveals that a typical user of online banking or Internet banking services can be classified as a highly educated, relatively young and wealthy person with a good knowledge of computers and especially the Internet (Karjaluoto et al., 2002, Al-Ashban and Burney, 2001) whereas having a good job and or occupation was not found significant. Many studies recognise that demographic characteristics impact on customer attitudes and behaviour concerning online banking (Alagheband, 2006; Lai and Li, 2005; Lassar et al., 2005; Eastin, 2002; Burke, 2002; Lee and Lee, 2001; Sathye, 1999).
2. Trust: is the customers' confidence in the bank's integrity and effectiveness in providing better electronic banking services to its users. Many researchers agree that trust is vital in online banking compared with offline banking as transactions of this nature contain sensitive financial information and people involved in the financial transaction have the feeling of insecurity about their access to important files and information transferred through the Internet such as credit card details (Alsajjan and Dennis, 2006). Further, Suh and Han (2002) consider the issue of trust as very important in online compared with offline banking. Customers' trust in their online transactions is important and has been identified as a key to the development of e-commerce (Yousafzai et al., 2003). We would assume that the feeling of insecurity or the lack of trust is common among bank customers, and therefore, the researcher would formulate the first hypothesis that *there are no significant trust differences among banks' customers in their use of electronic banking services*.
3. Security: Is the protection of bank customers when using the online banking transactions through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications in some countries. Electronic banking enables customers to handle their financial transactions from their own personal computers (PCs) or laptops that are connected to Internet. Customers can also use their cell phone, for example, to check their balance, transfer funds and pay bills. The ease of access and the convenience in using electronic banking services allow bank customers to conduct their banking transactions without having to speak to a customer service agent or visit their bank branch. Nonetheless, a number of security issues need to

be considered when using electronic banking services comprising identity theft, security breaches by Hackers. As a result, it is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by Hackers, banks need to adopt many security measures to ensure that customers information is protected (Quovardis, 2010). Basically there exist a number of different security methods for online banking including Personal Identification Number (PIN) system which represents a password used to login. Whereas Transaction Authentication Number (TAN), representing one-time passwords to authenticate financial transactions. TANs are a second layer of security above and beyond the traditional single-password authentication. TANs are supposed to give additional security since they operate as a way of two-factor authentication. Should the actual document or token containing the TANs be stolen, it will be of little use without the password. In contrast, if the login data are acquired, no transactions can be performed without a valid TAN (Riyad Bank, 2011). For additional security, the customer login requires authentication for reconfirmation of his identity. The most secure way of using TANs is to generate them by need using a security token or authentication using Mobile (Riyad Bank, 2011). As such, we would propose the second hypothesis that *there are no significant security differences among bank customers in their use of electronic banking services.*

Electronic banking services bring a radical change in the way commercial banks develop and maintain close relationships with their customers. The introduction of banking technology has made customers utilization of electronic banking services very significant. The study need to compare trust and security of electronic banking services in Saudi banks in considering both Saudi indigenous and Non Saudi expatriates, taking into account the demographics comprising age gender, education, and income. The study focuses on comparing trust and security of electronic banking services comprising ATMs, credit cards, telephone banking, mobile SMS, and Internet banking services between Saudis and Non Saudis.

METHODOLOGY

In collecting primary data from financial institutions, the researcher was aware that access issues pose constraints particularly when seeking information related to personnel, customers, investors and or financial data (Saunders et al., 1997, 2009). This study was necessarily exploratory as gaining access to banks in a complex environment of a developing country such as Saudi Arabia was a major research challenge (Al-Ashban and Burney, 2001; Sohail and Shaikh, 2007). As a result, the researcher used snowballing technique for data collection and closely worked to overcome problems of access in using his personal contacts as Bryman (2004, 2006, 2008) suggests a number of strategies for gaining access such as using friends, contacts, colleagues, and academics to help in gaining entry, in addition to getting support of a person within the institution to act as a promoter or a supporter (Bryman, 2006, 2008; Bryman et al., 2008, Mahdi, 2008).

To achieve the study objectives, a framework for data collection and analysis was used based on quantitative approach. Data were collected by means of snowballing technique. The snowballing technique is often used in populations which are difficult for researchers to approach such as the case of the females and the bank staff in Saudi Arabia. Questionnaires were distributed through employment of undergraduate research assistants to banks' respondents including Saudi and Non Saudi banks' customers. The quantitative approach aimed at testing the following null hypotheses:

1. That there are no significant trust differences between Saudis and Non Saudis in their use of electronic banking services in Saudi banks.
2. That there are no significant security differences between Saudis and Non Saudis in their use of electronic banking services in Saudi banks.

These hypotheses were addressed in data collected by the use of a questionnaire to provide quantitative data and an open ended question to provide qualitative data in seeking banks respondents' opinions. Questionnaire was formulated by reviewing relevant empirical studies so as to identify key variables and constructs based on the literature. Pilot study was conducted by testing and pre-testing the questionnaire in consultation with experts and 50 randomly selected banks' respondents. Feedbacks were incorporated and questions were then revised and refined. The final version of the questionnaire consists of 21 closed questions and one open ended question placed at the end of the questionnaire to allow for further comments and provide qualitative data in seeking banks respondents' opinions. Snap10 was used in the design of the questionnaire. Consequently, 500 copies of the questionnaire were distributed to bank respondents including faculty, managers, technicians, clerks, workers and students in Dhahran, Khobar, Damman and Jubail, which are considered the four big cities in the Eastern Province of the Kingdom of Saudi Arabia. The process of distributing and collecting data took six months. Eventually, 418 completed questionnaire copies were collected from respondents. Data were then filtered and 36 copies of questionnaire containing missing data were excluded from data entry, leaving 382 clean and fully completed questionnaire copies which represented 76.4 response rate. Reliability statistics test was conducted which yielded Cronbach's Alpha 0.786 and Cronbach's Alpha 0.754 based on standardized items (17 items) with an item mean score of 3.869. Questionnaire data were used to deduce the validity of research hypotheses in collecting responses from a pre-set series of questions (Bryman, 2008; Mahdi, 2008).

Initially, the study compared views of Saudi banks' customers against the Non Saudi banks' customers. The respondents' different viewpoints in trust and security of electronic banking services formed the basis for comparison and evaluation. The Statistical Package for Social Scientists (SPSS) for Windows package was utilised for the analysis of the data collected from the survey. The researcher used the means, variances and frequencies, in addition to independent-samples T-Test to test for statistical significance of the research hypotheses (Kinnear, and Gray, 1999: 171).

RESULTS AND DISCUSSION

Respondents' general profile

The findings from the study on trust and security of electronic banking services in Saudi banks are presented

Table 1. Respondents' demographics.

Demographic	Saudis (175)		Non Saudis (207)		Total (382)	
	N	Percent	N	Percent	N	Percent
Nationality	175	45.8	207	54.2	382	100
Gender						
Male	159	90.9	185	89.4	344	90.1
Female	16	9.9	22	10.6	38	9.1
Relationship with banks						
Bank customers	147	84	201	97.1	348	91.1
Bank staff	28	16	6	2.9	34	8.9
Age group						
Under 20	2	1.1	0	0	2	0.5
20-29	70	40	22	10.6	92	24.1
30-39	61	34.9	60	29	121	31.7
40-49	32	18.3	69	33.3	101	26.4
50-59	9	5.1	44	21.3	53	13.9
60 +	1	0.6	12	5.8	13	3.4
Educational level						
High School	33	18.9	7	3.4	40	10.5
Diploma	40	22.9	23	11.1	63	16.5
Bachelor	80	45.7	76	36.7	156	40.8
Master	12	6.9	54	26.1	66	17.3
Ph. D.	10	5.7	47	22.7	57	14.9
Income (SR)						
1000-5000	40	22.9	48	23.2	88	23
6000-10000	51	29.1	80	38.6	131	34.3
11000 - 15000	61	34.9	49	23.7	110	28.8
16000 - 20000	14	8	20	9.7	34	8.9
21000 +	9	5.1	10	4.8	19	5
Living area						
Ahsa	0	0	2	1	2	0.5
Dhahran	26	14.9	58	28	84	22
Khobar	18	10.3	45	21.7	63	16.5
Dammam	109	62.3	48	23.2	157	41.1
Jubail	11	6.3	53	25.6	64	16.8
Qatif	11	6.3	1	0.5	12	3.1

here. The findings about the respondents' general profile of Saudis and Non Saudis including age, gender, education, and income as displayed in Table 1 are also considered.

Table 1, shows the entire sample consists of (382) respondents of which (54.2%) 207 were Non Saudis, while (45.8%) 175 were Saudis. The findings reported how more than half of respondents were Non Saudis including expatriates working and residing in the Kingdom of Saudi Arabia, and nearly half of respondents were Saudi nationals participated in the study. In terms of gender, (90.1%) 344 were males, and only (9.9%) 38 were females. Vast majority of respondents were males and only few of them were females. This is not surprising, as the smaller number of female participated in the survey reflects an access problem and difficulties in

Table 2. Opinions on trust in electronic banking services.

Electronic banking service	Nationality	N	Mean	Std. deviation
ATMs	Saudi	173	5.55	0.632
Missing 10	Non Saudi	199	5.31	0.726
Credit cards	Saudi	143	4.94	1.067
Missing 122	Non Saudi	117	4.57	1.085
Mobile SMS	Saudi	107	5.10	0.961
Missing 196	Non Saudi	79	4.66	1.108
Phone banking	Saudi	129	5.19	0.864
Missing 174	Non Saudi	79	4.61	1.203
Internet banking	Saudi	149	5.12	1.026
Missing 110	Non Saudi	123	4.85	1.087
Trust degree	Saudi	175	5.21	0.701
Missing 3	Non Saudi	204	4.99	0.783

reaching females to collect primary data in a conservative environment such as Saudi Arabia. Saudi law does no allow direct contact and or interaction between male and females in general, and or between foreign males and Saudi females in particular. Sohail and Shaikh (2007) highlight that, in collecting primary data from Saudi Arabia 'legally and socially, females cannot be approached by male strangers' (Sohail and Kahtani, 2005).

Furthermore, (91.1%) 348 of respondents were bank customers, and only (8.9%) 34 were bank staff. Respondents were actually asked to describe their relationship either as a bank staff or a bank customer. Vast majority of respondents were bank customers and only few of them were bank staff. The few numbers of bank staff participated in the survey reflect some of constraints in getting entry to banks and difficulties in approaching bank staff to distribute questionnaires and collect data from Saudi banks. In many occasions, the researcher and his assistants were asked to obtain a written approval from the banks headquarters in Riyadh (the Capital of Saudi Arabia) prior to distributing the questionnaire in banks' branches in the Eastern Province of the Kingdom.

The overall results showed how the respondents were well educated (40.8 %, 156) had bachelor degrees, (17.3%) 66 had master degrees, (16.5%) 63 had diplomas and about (14.9%) 57 had Ph.D. degrees and only (10.5%) 40 had high school certificates. Findings revealed how the Non Saudi expatriates participated in the survey were highly educated as (26.1%) 54 and (22.7%) 47 of them hold Master and Ph.D. degrees compared with their counterpart (6.9%) 12 and (5.7%) 10 of Saudis who hold Master and Ph.D. degrees consecutively. Initially there was uncertainty that a questionnaire designed in English would not be understood and well answered particularly by indigenous respondents. The results reflected that the surveyed respondents were well educated and this has resulted in high response rate, generated useful data and reduced the cost of questionnaire translation from English into Arabic.

In terms of income, more than one third (34.3%) 131 of respondents had an income between 6000 and 10000 thousand Saudi Riyals (SR) per month, and more than a quarter (28.8%) 110 of respondents had income between 11000 and 15000 thousand SR per month. The results indicated how (23%) 88 of respondents had an income between 1000 and 5000 per month. Other respondents (8.9%) 34 had income between 16000 and 20000 per month. Only very few respondents (5%) 19 had an income more than 21 thousands SR per month. The income level was measured in Saudi Riyals (SR). During the study period (3.75) Saudi Riyals was equivalent to one (1) US$ Dollar.

As with regard to location of where these respondents live, about (41.1%) 157 of respondents reported that they live in Dammam. Less than a quarter (22%) 84 of respondents indicated that they live in Dhahran. About (16.8%) 64 and (16.5%) 63 showed that they live in Jubail and Khobar respectively. Very few (3.1%) 12 and (0.5%) 2 of respondents' survey revealed that they live in Qatif and Ahsa respectively. These results showed how the survey was very well conducted and that the questionnaires were distributed to targeted respondents in the four big cities in the Eastern Province of the Kingdom of Saudi Arabia, namely Damman, Dhahran, Jubail and Khobar that had generated reliable responses.

Table 3. Degree of trust in electronic banking services.

Electronic banking service		Levene's test for equality of variance		T-test for equality of mean		
		F	Sig.	T	Df.	Sig. (2- tailed)
ATMs	Equal var. assumed	2.876	0.091	3.494	370	0.001
	Equal var. not assumed			3.528	369.998	0.000
Credit cards	Equal var. assumed	0.185	0.668	2.771	258	0.006
	Equal var. not assumed			2.767	246.189	0.006
Mobile SMS	Equal var. assumed	2.972	0.086	2.921	184	0.004
	Equal var. not assumed			2.860	153.773	0.005
Phone b.	Equal var. assumed	11.988	0.001	4.026	206	0.000
	Equal var. not assumed			3.726	127.331	0.000
Internet b.	Equal var. assumed	0.156	0.693	2.144	270	0.033
	Equal var. not assumed			2.123	254.176	0.034
Trust Degree	Equal var. assumed	0.004	0.951	2.781	377	0.006
	Equal var. not assumed			2.804	376.335	0.005

Opinions on trust and security: Saudis versus non Saudis

Opinions on trust in electronic banking services

Table 2 describes the respondents' (Saudis and Non Saudis) opinions about their trust in any of the electronic banking services including ATM, credit card, mobile SMS, Phone banking and Internet banking. The degree of trust was measured applying Likert five scale from 'Very high' to 'Very low'. 'Never used' was treated as missing data and was excluded form the analysis.

Table 2 shows the mean score of (5.55) indicated how Saudis had very high trust in the electronic banking services namely the ATMs compared with the mean score (5.31) of their counterpart the Non Saudis. The findings suggested that Saudis had very high trust in the ATM compared with their counterpart the Non Saudis.

In terms of the Credit card, the mean score of (4.94) revealed how Saudis had high trust in the Credit cards compared with the mean score (4.57) of their counterpart the Non Saudis. The mean scores revealed that Saudis had high trust in the Credit cards compared with their counterpart the Non Saudis.

As for the Mobile SMS, the mean score (5.10) of Saudis indicated that they had high trust in the Mobile SMS than the (4.66) mean score of the Non Saudis. The findings considered that Saudis had very high trust in the Mobile SMS compared with Non Saudis.

With Phone banking, the mean score of (5.19) reported how Saudis have very high trust in the Phone banking compared with the mean score (4.61) of their counterpart the Non Saudis. The mean scores demonstrated that Saudis had very high trust in the Phone banking compared with Non Saudis.

Regarding Internet banking, the mean score (5.12) of Saudis indicated how they had high trust in the Internet banking compared with the mean score (4.85) of the Non Saudis who were using Internet banking. The findings suggested how Saudis had high trust in the Internet banking compared with Non Saudis.

Overall, the aggregate mean score of (5.21) revealed how Saudis had very high trust in using all electronic banking services namely ATMs, Credit cards, Mobile SMS, Phone banking and the Internet banking compared with the mean score (4.99) of their counterpart the Non Saudis.

Degree of trust in electronic banking services

Table 3 illustrates Saudis and Non Saudis degree of trust in electronic banking services in Saudi commercial banks including ATMs, Credit cards, Mobile SMS, Phone banking and the Internet banking. However, the null hypotheses had been presented for testing as follows:

H_0: that there are no significant trusts differences between Saudis and Non Saudis in their use of electronic banking services in Saudi banks.

H_1: that there are significant trust differences between Saudis and Non Saudis in their use of electronic banking services in Saudi banks

Table 4. Opinions about security of electronic banking services.

Electronic banking service	Nationality	N	Mean	Std. deviation
ATMs	Saudi	174	5.58	0.715
Missing 10	Non Saudi	198	5.23	0.765
Credit card	Saudi	143	4.83	1.183
Missing 126	Non Saudi	113	4.58	1.024
Mobile SMS	Saudi	105	5.28	0.814
Missing 201	Non Saudi	76	4.71	1.043
Phone banking	Saudi	132	5.26	0.853
Missing 172	Non Saudi	78	4.60	1.036
Internet banking	Saudi	150	5.17	0.988
Missing 107	Non Saudi	125	4.84	0.987
Security degree	Saudi	174	5.24	0.695
Missing 4	Non Saudi	204	4.96	0.766

The independent-samples t-test for statistical significance was used to test for significant trust differences in the electronic banking services between Saudis and Non Saudis in Saudi commercial banks applying $p<0.05$ as statistical level of significance. t-Test results (p-value 0.000, less than the critical value $p<0.05$) indicates highly significant differences.

Table 3 shows across the entire sample how there are highly significant trust differences in the electronic banking services between Saudis and Non Saudis in the commercial banking sector of Saudi Arabia in the Eastern Province. The findings suggested that, Saudis had high trust in using any of the electronic banking services comprising ATM, Credit cards, Mobile SMS, Phone and the Internet banking compared with less trust by their counterpart the Non Saudis (p-value 0.000, 0.006, 0.004, 0.000 and 0.033, respectively) in all electronic banking services indicated highly significant differences. The overall degree of trust among Saudis in using any of the electronic banking services (p-value 0.006) was significantly higher than their counterpart the Non Saudis.

Opinions on security of electronic banking services

Table 4 describes the respondents' (Saudis and Non Saudis) opinions about the security of electronic banking services including ATM, Credit card, Mobile SMS, Phone banking and Internet banking. The degree of security was measured applying Likert five scale from 'Very secure' to 'Not secure at all'. 'Never used' was treated as missing data and was excluded form the analysis.

Table 4 illustrates the mean score of (5.58) revealed how Saudis believed that the ATMs services are very secure compared with the mean score (5.23) of their counterpart the Non Saudis. The findings suggested that Saudis had very strong belief that the ATMs services are very secure compared with their counterpart the Non Saudis.

Regarding the Credit card, the mean score of (4.83) showed how Saudis thought that the Credit cards services are secure compared with the mean score (4.58) of their counterpart the Non Saudis who had less opinion about the security of Credit cards. The mean scores revealed that Saudis believed that the Credit cards services in the banking sector are secured compared with slightly less opinion about the security of their counterpart the Non Saudis.

With Mobile SMS, the mean score (5.28) of Saudis indicated that they considered that the Mobile SMS services are very secure compared with (4.71) mean score of the Non Saudis. The findings suggested that Saudis had strong belief that the Mobile SMS services are more secure than the opinions of the Non Saudis.

As for the Phone banking, the mean score of (5.26) reported how Saudis had very strong belief that the Phone banking services are very secure compared with the mean score (4.60) of their counterpart the Non Saudis. The mean scores indicated that Saudis believed how the Phone banking services are very secure compared with Non Saudis opinions.

In terms of the Internet banking, the mean score (5.17) of Saudis revealed how they considered that the Internet banking services are very secure compared with the mean score (4.84) of the Non Saudis who had less belief about the security of the Internet banking. The findings showed how Saudis had strong belief about the security of the Internet banking services compared with opinions of the Non Saudis.

Overall, the aggregate mean score of (5.24) revealed how Saudis have strong belief that the electronic banking services comprising ATMs, Credit cards, Mobile SMS,

Table 5. Security degree of electronic banking services.

Electronic banking service		Levene's test for equality of variance		t-test for equality of mean		
		F	Sig.	T	Df.	Sig. (2- tailed)
ATMs	Equal var. assumed	1.727	0.190	4.515	370	0.000
	Equal var. not assumed			4.535	368.605	0.000
Credit cards	Equal var. assumed	1.998	0.159	1.717	254	0.087
	Equal var. not assumed			1.746	251.848	0.082
Mobile SMS	Equal var. assumed	3.374	0.068	4.095	179	0.000
	Equal var. not assumed			3.937	136.597	0.000
Phone b.	Equal var. assumed	3.285	0.071	4.959	208	0.000
	Equal var. not assumed			4.718	137.961	0.000
Internet b.	Equal var. assumed	0.013	0.910	2.787	273	0.006
	Equal var. not assumed			2.787	264.238	0.006
Security degree	Equal var. assumed	0.119	0.730	3.666	376	0.000
	Equal var. not assumed			3.694	374.569	0.000

Phone banking and the Internet banking services are very secure compared with the mean score (4.96) of their counterpart the Non Saudis.

Security degree of electronic banking services

Table 5 describes the respondents' (Saudis and Non Saudis) opinions about the security of electronic banking services including ATM, Credit card, Mobile SMS, Phone banking and Internet banking. The null hypotheses had been presented for testing as follows:

H_0: There is no significant security difference between Saudis and Non Saudis in their use of electronic banking services in Saudi banks.

H_1: There are significant security differences between Saudis and Non Saudis in their use of electronic banking services in Saudi banks.

The independent-samples t-test for statistical significance was used to test for significant security differences of electronic banking services between Saudis and Non Saudis in Saudi commercial banks applying $p<0.05$ as statistical level of significance. t-Test results (p-value 0.000, less than the critical value $p<0.05$) indicates significant differences.

Table 5 shows across the entire sample how there are highly significant security differences in the electronic banking services between Saudis and Non Saudis in the commercial banking industry of the Kingdom. The findings suggested that, Saudis had strong belief that the electronic banking services are very secure compared with less belief about the security by their counterpart the Non Saudis (p-value 0.000, 0.000, 0.000, 0.006, respectively) in ATM, Mobile SMS, Phone and the Internet banking services indicated highly significant differences. Nevertheless, the findings (p-value 0.087) suggest that there are no significant differences between Saudis and Non Saudis in their judgement about the security of Credit cards services. However, the overall degree of security among Saudis in using any of the electronic banking services (p-value 0.000) is significantly higher than their counterpart the Non Saudis.

Moreover, a number of customers particularly the Non Saudis complained about the security of Credit cards. Respondents believed that Credit cards are not secure as the security code at the back of the cards can simply by read and copied by others as a bank customer commented:

'Any credit card should have a security number, but credit cards are not secure at all due to the fact that the three digit No. (Security code) can easily be read and used by others.'

Another security issue is related to the lack of use of Personal Identification Number (PIN) in shopping centres. In the Eastern Province of Saudi Arabia a customer can use his credit card to purchase from shopping centres without entering his PIN for verification. As a customer stated:

'Another problem is that we use our cards to buy form shops without using our PIN and this is a big problem because anyone can use your card, so I think PIN should be used along with credit cards in shopping centres.'

However, the Association for Payment Clearing Services

and card issuers, required customers to use the Chip and Pin by entering their personal identification number (PIN) on a special keypad located close to the Electronic Funds Transfer at Point of Sale Service (EPOS). The introduction of Chip and Pin System affected the vast majority of face-to-face transactions and removed the burden and responsibility of shop staff to confirm the identity of a cardholder and to compare the customer signature to that on the card. The introduction of PIN at EPOS reduced the level of fraud, decreased the amount of time it takes to process a credit/debit card transaction and therefore reduced the cost associated with processing cards for traders. Customers also no longer have to store copy vouchers for transactions that have been processed with chip and pin. In Saudi Arabia including the Eastern Province, the authorized credit card holders still do transactions in many shopping centres by signing a receipt rather than inserting their PIN.

With reference to Internet banking, a number of customers also complained about the security of electronic banking services particularly with Internet banking. Respondents believed that Internet banking is not secure as they encounter a number of security threats and use of their passwords in addition to the complexity of the security system as a bank customer commented:

'There are security threats with Internet banking. I find the Internet service is difficult to use and always I have a problem of my password being frozen and the Internet security procedures are too long and very complicated.'

Moreover, a number of security issues need to be considered when shopping online through the Internet such as identity theft, security breaches by Hackers, as a bank customer reported:

'I was stunned when I later discovered someone bought an airline ticket by Internet using my Credit card. This is unbelievable, I lost my money, and my bank was unable to help me or do anything for me.'

During the last few years, usage of the internet has expanded as a new way of online shopping across a wider range of merchants and products. Nevertheless, the potential for fraud has increased too. In 2001, Visa International introduced a new online payment programme as a way of keeping the card use secure on the internet. 3D internet security system for online purchasing using a credit card has been introduced. 3D is a secure way to pay online merchants as it verifies the credit cardholder's identity when shopping online. 3D adds security to online shopping protection as a customer knows that his transaction is protected, and the risk of fraud is reduced. Verification by Visa and Master Card Secure Code enable a cardholder to create a secret credential (such as a Password) that he or she will enter when shopping online as part of the check-out process. The Password is like an "electronic signature" for internet transactions. Once activated a card is Verified by Visa or Master Card Secure Code, and customer will be able to sign the transactions with his own secret Password just like signing the sales slip when shopping in person at a store. However, customers are required to enrol either through the bank's website or during their online shopping session with a participating merchant. As a result, it is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by Hackers, Saudi banks need to adopt many security measures to ensure that customers' information is protected

Conclusion

The study conducted in Saudi Arabia investigated and presented findings from survey data on the trust and the security of electronic banking services in Saudi banks in the Eastern Province of the Kingdom. The quantitative data presented very strong evidence to support the hypotheses *that there are significant trust differences between Saudi bank customers and Non Saudi bank customers in their use of electronic banking services including ATMs, Credit cards, Mobile SMS, Phone banking, and the Internet banking services in Saudi banks*. Independent t-test results (p-value 0.001, 0.006, 0.004, 0.000 and 0.033 respectively) indicate highly significant differences. The overall degree of trust among Saudis (p-value 0.005) was significantly higher than their counterpart the Non Saudi bank customers. Moreover, the quantitative data also presented very strong evidence to support the hypotheses that *there are significant security differences between Saudi bank customers and Non Saudi bank customers in their use of electronic banking services comprising ATMs, Credit cards, Mobile SMS, Phone banking, and the Internet banking services in Saudi banks*. Independent t-test results (p-value 0.000, 0.000, 0.000 and 0.006, respectively) indicate highly significant differences. The overall degree of security among Saudis bank customers in using any of the electronic banking services (p-value 0.000) was significantly greater than their counterpart the Non Saudis.

Bank respondents believed how the Credit cards are not secure and expressed their lack of trust in using Credit cards in shopping centres and the insecurity of these cards when shopping online via the Internet. The Non Saudi bank customers raised the issue of Credit cards security code. Bank respondents were sceptical about the use of their Credit cards as the three digits security code can easily be read, copied and used by others. Another security problem related to the lack of use of Personal Identification Number (PIN) in many Saudi shopping centres was also pointed out. In the Eastern Province of Saudi Arabia, bank customers use their Credit cards to purchase from big shopping centres without entering a PIN for verification, instead, the authorized Credit card holders still do transactions in

many shopping centres by signing a receipt rather than entering their PIN. Consequently, we would suggest that bank practitioners should address these security issues through the introduction and the implementation of Chip and PIN System, in order to remove the burden and responsibility of shop staff to confirm the identity of a cardholder and to compare the customer signature to that on the card. Accordingly, bank customers should no longer worry about storing copy vouchers for transactions that have been processed with Chip and PIN. Furthermore, it is very important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by Internet Hackers, Saudi banks need to adopt many security measures to ensure that customer's information is protected when shopping online through the Internet.

Considering Saudi banks together with Saudi-Foreign owned banks, along with customers' preferences of one bank on another, could have provided more evidence to support differences among banks' respondents. Nonetheless, in many occasions, the researcher and his assistants were faced with difficulties and constrained in getting entry to banks and in approaching banks' respondents to distribute questionnaires and or conduct interviews prior to obtaining a written approval from the banks' headquarters based in Riyadh (the Capital of Saudi Arabia).

Finally, we would argue that the insufficiency of literature in the area of electronic banking services and the banking technology in developing countries becomes central for academics to conduct further research in this field. The bulk of the studies on banking technology services are based in mature industrial countries with a well-developed infrastructure, extensive education system, and relatively stable political economy. A further study in developing countries mainly in the Middle East that examines this area of technology is considered to be crucial; for example, the issue of gender on the usage of electronic services is an area in need of further investigation. In the context of Saudi Arabia, researchers are also urged to further examine the issues of electronic banking technology services in relation to gender. We would also suggest further research in Saudi banks, should consider customer's preference of one bank on another.

ACKNOWLEDGMENTS

The author would like to acknowledge the financial support provided by the Deanship of Scientific Research at King Fahd University of Petroleum and Minerals (KFUPM) under Research Grant Number IN100012. Am also grateful to all research assistants who helped in data collection and technicians who assisted in data entry and data analysis.

REFERENCES

Alagheband P (2006). Adoption of electronic banking services by Iranian customers. Master Thesis, University of Technology, Sweden, Lulea.

Al-Ashban AA, Burney MA (2001). Customer adoption of tele-banking technology: the case of Saudi Arabia. Int. J. Bank Mark., 19(5): 191-200.

Alsajjan B, Dennis C (2006). The Impact of trust on acceptance of online banking. In: European Association of Education and Research in Commercial Distribution. Brunel University. West London, United Kingdom, 27-30 June.

Al-Somali SA, Gholami R, Clegg B (2009). An investigation into the acceptance of online banking in Saudi Arabia. Retrieved20 December 2009. Available at: http://www. Sciencedirect.com. and also www.elsevier.com/locate/technovation. Technovation, 29: 130-141.

Al-Sukkar AS (2005). The Application of Information Systems in Jordanian Banking Sector, a Study of the Acceptance of the Internet. Thesis (Ph. D.), Australia: University of Wollongong.

Bauer HH, Hammershmidt M, Falk T (2005). Measuring the quality of e-banking portals. Int. J. Bank Mark., 23(2): 153-75.

Bryman A (2004). Social Research Methods (2nd edn): Oxford University Press.

Bryman A (2006). 'Integrating Quantitative and Qualitative Research: How is it Done?' Qual. Res., 6(1): 97-113

Bryman A (2008). Social Research Methods (3rd edn): Oxford University Press.

Bryman A, Saul B, Joe S (2008). Quality Criteria for Quantitative, Qualitative and Mixed Methods Research: A View from Social Policy. Int. J. Soc. Res. Methodol., 11(4): 261-276

Burke RR (2002). Technology and the customer interface: what consumers want in the physical and virtual store? J. Acad. Mark. Sci., 30(4): 411-432.

Childs JB (1994). The Impact of Technology on Foreign Exchange. Bank. Mag., 28-33.

Dabholkar P, Bagozzi R (2002). "An attitudinal model of technology-based self-service: moderating effects of consumers traits and situational factors". J. Acad. Mark. Sci., 30(3): 184-201.

Davis DF (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. MIS Q., 13(3): 319-40.

Dixon P (2002). Future of Banking – Expectations January 2002. Impact of new Technology on Banking and Financial Services. Retrieved: 03rd October 2009. Available at: http://www.globalchange.com/futurebank.html

Eastin M (2002). Diffusion of e-commerce: an analysis of the adoption of four e-commerce activities. Telematic Inform., 19(3): 251–267.

EIA Energy Information Administration (2011), U.S. Department of Energy, Saudi Arabia, Country Analysis Brief, Available at: http://www.eia.doe.gov/ countries/country-data.cfm?fips=SA. Accessed: 8th April, p. 32.

Harris L (2001). The IT Productivity Paradox-Evidence from the UK Retail Banking Industry. UK and Boston, Oxford, Blackwell Publishers Ltd. New Technol, Work Employ. March, 16(1): 35-48).

Hellriegel D, Jackson SE, Slocum JW Jr. (2005). Management: A Competency Based Approach. 10th edn, Ohio, South Western.

Karjaluoto H, Mattila M, Pento T (2002). Factors underlying attitude formation towards online banking in Finland. Int. J. Bank Mark., 20(6): 261-272.

Kinnear PR, Gray CD (1999). SPSS for Windows Made Simple, (3rd edition). England: East Sussex. Psychology Press Ltd, Publishers, 171.

Kripanont N (2007). Examining a Technology Acceptance Model of Internet Usage by Academics within Thai Business Schools. Thesis (Ph.D.), Melbourne, Australia: Victoria University.

Lai VS, Li H (2005). Technology acceptance model for internet banking: an invariance analysis. Inform. Manage., 42(2): 373-386.

Lassar WM, Manolis C, Lassar SS (2005). The relationship between consumer innovativeness, personal characteristics, and online banking adoption. Int. J. Bank Mark., 23(2): 176–199.

Lee E, Lee J (2001). Consumer adoption of internet banking: need-based and/or skill based. Mark. Manage. J., 11(1): 101-113.

Lee G, Lin H (2005). Customer perceptions of e-service quality in online shopping. Int. J. Ret. Distrib. Manage., 33(2): 161-76.
Mahdi MOS, Dawson P (2007). The Introduction of Information Technology in the Commercial Banking Sector of Developing Countries: voices from Sudan. J. Inform. Technol. People (ITP). 20(2): 184-204.
Mahdi MOS (2008). The value of multi-strategy research methodology in conducting fieldwork study into information technology implementation in Sudanese banks. J. Sci. Technol., 9(1): 127-146.
Marlin S (2004). Banks to Boost Spending on New Technology for Branches: Information Week, January 20, 2004. Retrieved: 03rd October 2009. Available at: http://www.informationweek.com/showArticle.jhtml
Parasuraman A, Zinkhan GM (2002). Marketing to and serving customers through the Internet: an overview and research agenda. J. Acad. Mark. Sci., 30(4): 286-95.
Quovardis R (2010) Security Issues with Online Banking, eHow.com. Available at: http://www.ehow.com/list_5950326_security-issues-online-banking.html, Accessed: 09th November 2010
Riyad bank (2011) Riyadonline.com, Available at: https://www.riyadonline.com./detect.jsp. Accessed: 17th March.
Sathye M (1999). Adoption of internet banking by Australian consumer: an empirical investigation. Int. J. Bank Mark, 17(7): 324-334.
Saunders M, Lewis P, Thornhill A (1997). Research Methods for Business Studies. London: Pearson Professional Limited.
Saunders M, Thornhill A, Lewis P (2009). Research Methods for Business Students, (5th edn). Publisher: Financial Times Press.
Slocum JW Jr., Jackson SE, Hellriegel D (2008). Management: A Competency Based Approach. 11th edn, Ohio, South Western.
Sohail MS, Kahtani A (2005). Measuring service quality at King Fahd International Airport. Int. J. Serv. Standard, 1(4): 482-493.
Sohail MS, Shaikh NM (2007). Internet banking and quality of service, perspectives from a developing nation in the Middle East. Online Info. Rev., 32(1): 58-72.
Suh B, Han I (2002). Effect of trust on customer acceptance of Internet banking. Electron. Com. Res. Appl., 1(3): 247-263.
Venkatesh V, Davis FD (2000). A theoretical extension of the Technology Acceptance Model: four longitudinal field studies. Manage. Sci., 46(2): 186-204.
Venkatesh V, Morris MG, Davis GB, Davis FD (2003). User acceptance of Information Technology: toward a unified view. MIS Q., 27 (3): 425-78.
Yousafzai SY, Pallister JG, Foxall GR (2003). A proposed model of e-trust for electronic banking. Technovation, 23(11): 847-860.
Zeithaml VA (2002). Service-excellence in electronic channels, Managi. Serv. Qual., 12(3): 135-48.
Zeithaml V, Parasuraman A, Malhotra A (2000). e-Service quality: definition, dimensions and conceptual model, working paper. Marketing Science Institute. Cambridge, MA.
Zeithaml V, Parasuraman A, Malhotra A (2002). Service quality delivery through websites: a critical review of extant knowledge. Acad. Mark. Sci. J., 30(4): 362-75.
Zhang X, Prybutok VR (2005). A consumer perspective of e-service quality. IEEE Trans. Eng. Manage., 53(4): 461-77.