ISSN No:-2456 –2165

Investigation of How E-Risk Deters E-Readiness of Banks in Ghana

Carlo K.M.H. Adadevoh, Agyenna kesse-Tachi, Prof. Ntim

Abstract :There are inherent risks in banking which makes it necessary to investigate e-risk in the banking industry. Risk particularly deters customers, making e-risk one of the factors that determine whether a bank gets ready to adopt e-commerce. The study collected data from banks in the Greater Accra Region and used the principal component analysis to test whether all or some of the e-risk variables deter e-readiness in the banking industry. The study concluded that fourteen e-risk variables deter banks e-readiness. These variables included outsourcing, unauthorized access to a web site, and retrieval of confidential customer information by hackers, interruption of service provider's, loss of customers among others. Therefore, for banks to manage e-risk, they must endeavor to implement security policies and measures, coordinate internal communication, evaluate and upgrade products and services regularly and test systems operations regularly.

Keywords:- e-commerce, e-banking, e-risks, e-assets.

I. INTRODUCTION

ICT comprises of ICT infrastructure, hardware, software, and the people to utilise them. It is used to create, distribute, store and manage information (Chanyagorn & Kungwannarongkun , 2011). ICT and technological development has brought much change to business processes over the years, affecting the conduct of almost every activity, including banking (Bui, Sankaran, & Sebastian, 2003; Chanyagorn&Kungwannarongkun, 2011; Patel, Patel, Ganatra, &Kosta, 2017). However, the use of ICT in e-commerce exposes such systems to risks during transactions (Fianyi, 2015; Solanki, 2012). The presence of e-risks influences companies in terms of the system the company will operate with, the services it can provide, or discourages the company entirely from engaging in e-commerce (Pezderka & Sinkovics, 2011).

II. E-COMMERCE

A consequence of ICT development is that e-commerce has become an indispensable component of the global market through which economic activities are conducted (Bui, Sankaran, & Sebastian, 2003; Fianyi, 2015; Smith, 2008). E-commerce involves the purchase and supply of goods and services using an electronic medium for the transaction (Anamuah-Mensah&Marfo, 2009; Boateng, Molla, Heeks, & Hinson, 2011; Patel, Patel, Ganatra, &Kosta, 2017; Turban, Lee, King, & Chung, 1999). The development of the World Wide Web in the 1990s is considered to have made the conduct of e-commerce possible (Smith, 2008). Due to e-commerce, the global economy is now conducted in real time with little to no challenges in relation to time, physical location and accessibility of goods and services (Bui, Sankaran, & Sebastian, 2003).

This is made possible by internet-based networking and integration, which allows for service provision across traditional physical boundaries (Bui, Sankaran, & Sebastian, 2003). Its relative reliability and efficiency has made it an essential component of trade, and has become a preferred business transaction method in this global dispensation (Smith, 2008). In the pursuit of e-commerce, the e-assets of a company are significant in the ability to partake in e-commerce (Pezderka & Sinkovics, 2011). E-assets comprise investments in the IT infrastructure and the human resources of the company that enables the company to function effectively in an e-commerce environment, as well as give it a competitive advantage (Pezderka & Sinkovics, 2011).

III. E-BANKING

Companies are increasingly adopting ICT as a strategic tool within their respective competitive markets (Pezderka & Sinkovics, 2011). Not only does it help companies survive, but also provides an avenue for such companies to access international opportunities (Pezderka & Sinkovics, 2011). The role of banks in transactions is to provide financial flow services (Gobat, 2012). Electronic banking involves the provision of banking products and services using an electronic medium (Basel Committee on Banking Supervision, 1998; Liébana-Cabanillas, Muñoz-Leiva, & Rejón-Guardia, 2013). E-banking has been reported to improve the speed, convenience and cost of service provision of banks to its customers (Solanki, 2012).

The use of e-banking is also considered to significantly reduce human errors and fraud that is associated with traditional/manual banking practices (Basel Committee on Banking Supervision, 2001). With these positives, e-banking has the potential to move from a complementary system to traditional banking practices, to the main form of banking practice over time (Solanki, 2012). Failure of banks to take advantage of e-banking opportunities therefore is likely to negatively their chances to effectively compete in the ever evolving banking industry (Solanki, 2012). The practice of e-banking is however exposed to some challenges that threaten the system (Fianyi, 2015; Solanki, 2012). This means that banks must have systems that allows it to manage the risks they currently face, and which is also

able to adjust itself in response to the emergence of newer risks (Basel Committee on Banking Supervision, 1998).

IV. E-RISKS

Potential financial and technological challenges that emerge when engaging in e-commerce are known as e-risks (Patel, Patel, Ganatra, &Kosta, 2017; Smith, 2008). Identification of e-risks has sometimes been based on perceptions of the e-business environment, instead of its realities (Pezderka & Sinkovics, 2011). In addition, some assessments of e-risks have not necessarily been based on how a company can internationalize its operations, but rather how it can make an entry into existing traditional markets (Pezderka & Sinkovics, 2011).

Risks to traditional banking practices include credit, liquidity, interest rate, operational, reputational, or legal risks (Basel Committee on Banking Supervision, 1998). Of these, risks most common to e-banking are operational, reputational, security, and legal risks, among others (Basel Committee on Banking Supervision, 1998; Solanki, 2012). The following include some risks to e-commerce:

A. Operational Risks

Operational risks occurs when a bank is unable to provide e-services to clients and are associated with processing errors, system disruptions, and fraud (Basel Committee on Banking Supervision, 1998; Solanki, 2012). E-banking is heavily reliant on the use of ICT tools (Basel Committee on Banking Supervision, 2001; Solanki, 2012). This overdependence makes the entire system susceptible to operational challenges in situations where there is a breakdown of the ICT tools or the medium of transaction (e.g. internet interruption) (Basel Committee on Banking Supervision, 2001). The introduction of viruses to information systems can also deny access to or corrupt information that is needed to provide services to clients (Solanki, 2012). In addition, the use of systems considered inadequate to the requirements of clients of the bank can result in system performance delays or disruptions (Basel Committee on Banking Supervision, 1998).

B. Security Risks

Online transactions sometimes involve the disclosure of confidential information over the net as part of transaction requirements (Fianyi, 2015). The anonymous nature of transactions makes it possible for the submission of false information during transactions (Solanki, 2012). The ‘open’ nature of the internet exposes electronic transactions to interceptions over the internet (Pezderka&Sinkovics, 2011; Smith, 2008). The challenges these present include theft, privacy violation, system intrusions and financial espionage (Fianyi, 2015; Smith, 2008). E-banking theft occurs when an individual hacks into a banking system to divert funds (Patel, Patel, Ganatra, & Kosta, 2017). With espionage, hackers sell confidential information about clients to others for extortion purposes (Patel, Patel, Ganatra, & Kosta, 2017). Theft can emanate from individuals outside the banking institution, or from bank employees who due to their knowledge of the security system seek to take advantage of their access to perpetuate crime against the bank. These have been made possible by improvement in tools (hardware and software) used in hacking into such systems, also a product of ICT improvement (Fianyi, 2015).

C. Reputational Risks

Risks to reputation involve the generation of negative impressions for a banking institution (Basel Committee on Banking Supervision, 1998). Lapses in service provision such as a breach of the banks security system or undue service delays where clients are not given adequate information largely contributes to this. The impact of this is the loss of clients (current and potential) and its financial consequences. Any divulgence of client information may have its own legal implications, in addition to the loss of client base of the bank due to the damage that such occurrence does to its reputation. The effects of these challenges are the loss of data (of both client and bank), computer system breakdown, as well as costs associated with repairs and legality issues (Solanki, 2012).

D. Time Risks

The limited time within which to properly assess newer technologies is a risk to e-banking (Basel Committee on Banking Supervision, 2001). Previously, the introduction of banking systems to clients was done only after extensive testing. Presently, the need to remain competitive denies banks the opportunity to adequately test newer banking systems/services before introducing it to clients (Basel Committee on Banking Supervision, 2001). This practice prevents the conduct of proper risk assessments on the products.

These risks occur because continuous technological improvements means there is no end to the type of challenges that emerges along the way (Solanki, 2012). The manifestation of e-risks with time is reported to have resulted in the loss of money, clients and reputation (Smith, 2008). E-risks compromises computer systems and prevent service providers to attend to the needs of their clients. Existing and potential clients may lose trust in a company whose e-commerce system has been compromised. Dissatisfied clients may seek services elsewhere and this leads to the loss of client base. These ultimately have financial implications, while funds can directly be stolen online through diversion, identity theft, and the sale of sensitive information through blackmails. Despite this challenge, Solanki (2012) indicates that technology still holds the key in solving these challenges by providing counter measures that offers some protection (Pezderka&Sinkovics, 2011; Solanki, 2012).

V. E-READINESS, E-BANKING AND E-RISKS IN GHANA

E-readiness shows the competency levels of a system to use ICT in transforming traditional business practices to conform to that of e-commerce (Bui, Sankaran, & Sebastian, 2003). Support for e-commerce development varies across countries, with differences in the capacities of countries to partake in e-commerce directly influencing their level of competitiveness at the global level. By extension, the e-readiness of a country has an influence on the e-performance of the local industries in that country (Bui, Sankaran, & Sebastian, 2003).

Innovation in technology and the competitive nature of the banking industry has resulted in the introduction of various electronic services and products (Basel Committee on Banking Supervision, 2001). Ghana's banking sector has witnessed significant developments including the provision of e-banking services over the years, through both direct and indirect efforts (Adams &Lamptey, 2009; Asante-Gyabaah, Oppong, &Idun-Baidoo, 2015; Boateng, Molla, Heeks, & Hinson, 2011). Associated with these developments are risks to e-banking in general, and it is imperative for banking institutions to recognize and take measures to address the potential risks.

Addressing the challenges of risks to e-banking require the conduct of risk assessments (Nastase & Nastase, 2007). Risk assessments involves identification of possible sources of challenges to a system, its potential impacts, as well as possible measures which can be used to either prevent or mitigate the challenges (Nastase & Nastase, 2007). An assessment of these challenges has implications for both country and company (Pezderka & Sinkovics, 2011). First, the ability to identify and manage e-risks as a conscious activity becomes an asset to the company/country in terms of its ability to operate in an e-commerce environment. Secondly, the lack of this capability has the potential to lead to the collapse of the company in the event that e-risks are encountered. Thirdly, the level of e-risks present in a country influences the nature of e-transactions (i.e. services and products) that would be adopted by industries in that country (Pezderka & Sinkovics, 2011). This paper therefore seeks to explore the risks to e-banking, particularly if e-risks influence the e-readiness of banks in Ghana.

VI. METHODOLOGY

The target population of this study will be banks in Ghana, specifically those located in the Greater Accra region, which is the region of study. Primary data would be obtained through the conduct of in-depth interviews with identified representatives of the bank. The tool for data collection would be a semi-structured questionnaire, the results of which would be presented under themes and discussed relative to literature. The study used principal component analysis to test whether all or some of the e-risk variables deter e-readiness in the banking industry. Principal Component Analysis is used to identify patterns in data, and it expresses the data in such a way as to highlight their similarities and differences.

VII. DATA ANALYSIS

This section presents the presentation, data analysis and discussion of results. The first section presents the preliminary analysis of the data and the second section shows further analysis using principal component analysis.

	Frequency	Percent
Bachelor's degree	101	43.5
Post-graduate degree	74	31.9
Professional	57	24.6
Total	232	100.0

Table 1: Edcational Level of Repondents

Table 1 shows the educational level of respondents. The table reveals that one hundred and one (101) of the respondents constituting 43.5% hold bachelor's degree, seventy-four (74) of the respondents constituting 31.9% hold post-graduate degree and fifty-seven (57) of the respondents constituting 24.6% hold professional certificate.

	Frequency	Percent
1-3 years	10	4.3
4-6 years	90	38.8
7-10 years	132	56.9
Total	232	100.0

Table 2: Number of years in banking in operation

Table 2 present the number of years' banks have been in operation. From the table above about 57% of the respondents indicated that their banks have been in operation for 7 to 10 years, 38.8% indicated that their banks have been in operation for 4-6 years and 4.3% indicated that their banks have been in operation for 1 to 3 years.

	Frequency	Percent
1-3 years	56	24.1
4-6 years	142	61.2
7-10 years	34	14.7
Total	232	100.0

Table 3: Length of service

Table 3 shows the length of service of respondents in the banking sector. As shown in the table above, about 61.2% of the respondents have worked in the banking industry for 4 to 6 years, 24.1% indicated that they have worked in the banking industry for 1 to 3 years and about 15% have worked in the banking industry for 7 to 10 years.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.770
Bartlett's Test of Sphericity	Approx. Chi-Square	1422.496
	Df	231
	Sig.	.000

Table 4: KMO and Bartlett's Test

From the table above, KMO obtained a value of 0.770 (which is greater than the minimum threshold of 0.50 (Sharma, 1996) suggesting that the sample size is adequate. Also the Bartlett's test of 0.000 suggest that some of the variables are inter-correlated and hence the data is suitable for Principal component analysis.

Table 5 present the result on the principal components extracted based on the eigenvalue criterion. Based on the eigenvalue, six principal components were extracted. This six-component accounted for 71.07% (which is above the threshold of 70%) of the variations in the dataset. The first component has the highest eigenvalue of 7.735 and accounted for most of the variation in the data sets (35.2%). The second component also obtained an eigenvalue of 2.196, accounting for 9.98% of the variation which was not accounted by the first component. The third principal components extracted accounted for 8.46% variation in the dataset. The fourth, fifth and sixth components extracted accounted for 6.66%, 5.89% and 4.93% variations in the dataset respectively. The result clearly suggests that the six-component extracted in this study are good enough to represent the e-risk factors that affect e-readiness. It is important to however mention that component one explained 35% of the variance in the dataset, hence can represent e-risk factors that affect e-readiness in further analysis.

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7.735	35.160	35.160	7.735	35.160	35.160
2	2.196	9.980	45.140	2.196	9.980	45.140
3	1.861	8.457	53.597	1.861	8.457	53.597
4	1.465	6.659	60.257	1.465	6.659	60.257
5	1.295	5.888	66.144	1.295	5.888	66.144
6	1.084	4.926	71.070	1.084	4.926	71.070
7	.924	4.201	75.271			
8	.884	4.017	79.288			
9	.703	3.194	82.482			
10	.640	2.908	85.391			
11	.592	2.690	88.081			
12	.478	2.174	90.255			
13	.381	1.731	91.986			
14	.333	1.512	93.498			
15	.287	1.303	94.801			
16	.258	1.171	95.972			
17	.243	1.103	97.075			
18	.192	.874	97.949			
19	.143	.650	98.600			
20	.129	.584	99.184			
21	.109	.496	99.680			
22	.070	.320	100.000			

Extraction Method: Principal Component Analysis.

Table 5: Extracted Principal Components Based on the Eigen value Criterion

	Component					
	1	2	3	4	5	6
Volume forecast: banks in the Internet environment have challenges on how to predict and manage the volume of customers.						.790
Difficulties in obtaining adequate management information to monitor e-services				-.549		
Outsourcing: banks offering e-banking services outsource related business functions like security and this can cause material risk.	.483					
Credit card information intercepted in transit is disclosed or used for fraudulent purposes					-.550	
After unauthorized access to a web site, online information about employees or customers is stolen, damaged or	.552					
Intercepting and copying or changing non-credit card information during transmission					.611	
Hackers operating via the Internet could access, retrieve and use confidential customer information and also can implant virus.	.483					
Bank is exposed to the risk of an interruption or slow-down of its existing systems if the electronic banking or electronic money system it chooses is not compatible with user requirements.		.527				
A service provider's operations could be interrupted due to system breakdowns or financial difficulties, jeopardizing a bank's ability to deliver products or services.	.568					
Rapid technological change can mean that staff may fail to understand fully the nature of new technology employed by the bank			.720			
Affected customers may leave the bank and others may follow if the	.699					

Losses to similar institution offering same type of services causing	.930					
Targeted attacks on a bank like hacker spreading inaccurate information about bank products.	.801					
A virus disturbing bank's system causing system and data integrity problems	.831					
Banks expose themselves to the money laundering risk.	.721					
Money laundering may result in legal sanctions for non-compliance with "know your customer" laws.		.068				
There can be a lack of understanding among senior management about its potential and implications.	.621					
People with technological, but not banking, skills can end up driving the initiatives.	.786					
E-initiatives can spring up in an incoherent and piecemeal manner in firms.	.599					
Credit risk	.753					
Market risk	.619					
Interest rate risk		.645				

Extraction Method: Principal Component Analysis. a. 6 components extracted.

Table 6: Loadings on the Principal Components

From Table 6, principal component one loaded fourteen (14) variables identified in the literature (Fianyi, 2015; Solanki, 2012; Pezderka & Sinkovics, 2011). These included outsourcing, unauthorized access to a web site,retrieval of confidential customer information by hackers, interruption of service provider's, loss of customers, spreading inaccurate information about bank products,loss to similar institution offering same type of services, targeted attacks on a bank like hacker,virus disturbing bank's system causing system and data integrity problems, banks expose themselves to the money laundering risk, lack of understanding among senior management, e-initiatives can spring up in an incoherent and piecemeal manner in firms, credit risk, market risk and people with technological, but not banking, skills can end up driving the initiatives. Table 6 also showed that component two loaded three variables and they are: Bank is exposed to the risk of an interruption or slow-down of its existing systems, money laundering and interest rate risk. Component three and four retained one variable and they are failure by staff to understand fully the nature of new technology employed by the bank and difficulties in obtaining adequate management information to monitor e-services respectively. The fifth component retained two variables: credit card information intercepted by fraudsters and intercepting and copying or changing non-credit card information during transmission. Component six loaded only one variable: challenges in volume forecast.

Table 7 present the results on managing e-risk. It can be observed that generally respondents agreed that implementing security policies and measures (M = 3.60, SD =0.564), co-coordinating internal communication (M = 3.70, SD = 0.680), evaluating and upgrading products and services (M = 3.93, SD =0.821), Testing of systems operations regularly can help detect unusual activity patterns and avert major system problems, disruptions, and attacks (M = 3.75, SD =0.607) are ways of managing e-risk in the banking industry.

Managing e-risk	**Mean**	**Std. Deviation**
Implementing security policies and measures	3.60	0.564
Co-coordinating internal communication	3.70	0.651
Evaluating and upgrading products and services	3.67	0.680
Implementing measures to ensure that outsourcing risks are controlled and managed	3.93	0.821
Providing disclosures and customer education	2.79	0.896
Developing contingency plans: contingency plan may address data recovery, alternative data-processing capabilities, emergency staffing, and customer service support.	2.68	0.569
Senior management should ensure that staffs responsible for enforcing risk limits have authority independent from the business unit undertaking the electronic banking or electronic money activity	2.52	0.801
Testing of systems operations regularly can help detect unusual activity patterns and avert major system problems, disruptions, and attacks.	3.75	0.607

Table 7: Managing e-risk

VIII. DISCUSSION OF RESULT

The study sought to identify the e-risk factors that deter e-readiness in the banking industry. The findings from the study revealed that six principal components extracted identify the e-risk factors. However, it was observed that component one explained most of the variations in the e-risk factors, hence was used to represent the e-risk factors which deter e-readiness. These e-risk factors identified are outsourcing, unauthorized access to a web site,retrieval of confidential customer information by hackers, interruption of service provider's, loss of customers, spreading inaccurate information about bank products,loss to similar institution offering same type of services, targeted attacks on a bank like hacker,virus disturbing bank's system causing system and data integrity problems, banks expose themselves to the money laundering risk, lack of understanding among senior management, e-initiatives can spring up in an incoherent and piecemeal manner in firms, credit risk, market risk and people with technological, but not banking, skills can end up driving the initiatives. The result suggests that these fourteen variables are factors that deter banks to be e-ready. This finding is consistent with the studies by Solanki (2012) who found that these fourteen factors affect banking industry. It is also consistent with the findings of Miller (1999).

The study also revealed that implementing security policies and measures, coordinating internal communication, evaluating and upgrading products and services and testing of systems operations are ways of managing e-risk in the banking sector. These findings are in agreement with findings of Solanki (2012) who found that e-risk is better managed through the implementation of security policies and measures, co-coordinating internal communication and evaluating and upgrading products and services. The finding is also consistent with the findings of Miller (1999).

IX. CONCLUSION

The study sought to examine the e-risk factors that deter banks e-readiness. Based on the analysis it was revealed that fourteen e-risk variables deter banks e-readiness. These variables are outsourcing, unauthorized access to a web site,retrieval of confidential customer information by hackers, interruption of service provider's, loss of

customers, spreading inaccurate information about bank products,loss to similar institution offering same type of services, targeted attacks on a bank like hacker,virus disturbing bank's system causing system and data integrity problems, banks expose themselves to the money laundering risk, lack of understanding among senior management, e-initiatives can spring up in an incoherent and piecemeal manner in firms, credit risk, market risk and people with technological, but not banking, skills can end up driving the initiatives. Also, the study found that to manage e-risk in the banking sector, banks must endeavor to implement security policies and measures, coordinate internal communication, evaluate and upgrade products and services regularly and test systems operations regularly. Following from this study, future research may be conducted on the e-risk factors that deter customers from patronizing banks e-services.

REFERENCE

[1]. Adams, A., & Lamptey, A. (2009). Customer perceived value in internet banking in Ghana. . Winneba: University of Education.

[2]. Anamuah-Mensah, E., & Marfo, G. (2009). E-Business Adoption in the Banking Industry in Ghana. Lulea: Lulea University of Technology.

[3]. Asante-Gyabaah, G., Oppong, C. N., & Idun-Baidoo, N. (2015). Electronic Banking in Ghana: A Case of GCB Bank Ltd. European Journal of Business and Management, 7(12), 239-256.

[4]. Basel Committee on Banking Supervision. (1998). Risk management for electronic banking and electronic money activities. Bank for International Settlements. Basel: Bank for International Settlements.

[5]. Basel Committee on Banking Supervision. (2001). Risk Management Principles for Electronic Banking. Basel: Bank for International Settlements.

[6]. Boateng, R., Molla, A., Heeks, R., & Hinson, R. (2011). Advancing E-commerce Beyond Readiness in a Developing Economy: Experiences of Ghanaian Firms. Journal of Electronic Commerce in Organizations, 9(1), 1-16.

[7]. Bui, T. X., Sankaran, S., & Sebastian, I. M. (2003). A framework for measuring national e-readiness. International Journal of Electronic Business, 1(1), 3-22.

[8]. Chanyagorn , P., & Kungwannarongkun , B. (2011, June 11). ICT Readiness Assessment Model for Public and Private Organizations in Developing Country. International Journal of Information and Education Technology, 1(2), 99-109.

[9]. Fianyi, I. D. (2015, November). Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics . nternational Journal of Computer Science Issues , 12(6), 78-85.

[10]. Gobat, J. (2012). What Is a Bank? Finance & Development, 49(1), 38-39.

[11]. Liébana-Cabanillas, F., Muñoz-Leiva, F., & Rejón-Guardia, F. (2013). The determinants of satisfaction with e-banking. Industrial Management & Data Systems, 113(5), 750-767.

[12]. Miller, H. (1999). Managing risks in electronic commerce.

[13]. Nastase, F., & Nastase, P. (2007). Risk Management for e-Business . Revista Informatica Economică , 3(43), 56-59.

[14]. Patel, M., Patel, N., Ganatra, A., & Kosta, Y. (2017). E-Commerce with Attached E-Risk with Cyber Crime. Retrieved May 15, 2017, from www.researchgate.net: http://www.researchgate.net/publication/265202079_E-Commerce_and_Attached_E-Risk_with_Cyber_crime

[15]. Pezderka, N., & Sinkovics, R. (2011). A conceptualization of e-risk perceptions and implications for small firm active online internationalization. International Business Review(20), 409-422.

[16]. Smith, K. (2008, December). An Analysis of E-Commerce: E-Risk, Global Trade, and Cybercrime. Retrieved May 15, 2017, from www.researchgate.net: http://ssrn.com/abstract=1315423

[17]. Solanki, V. S. (2012, September). RISKS IN E-BANKING AND THEIR MANAGEMENT. International Journal of Marketing, Financial Services & Management Research , 1(9), 164-178.

[18]. Turban, E., Lee, J., King, D., & Chung, H. M. (1999). Electronic Commerce: A Manag*erial Perspective.* New Jersey: Prentice Hall.