JISTEM - Journal of Information Systems and Technology Management
Revista de Gestão da Tecnologia e Sistemas de Informação
Vol. 11, No. 3, Sept/Dec., 2014 pp. *533-548*
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752014000300002

DETERMINING FACTORS OF BANK EMPLOYEE READING HABITS OF INFORMATION SECURITY POLICIES

William Allassani
University of Professional Studies, Legon-Accra, Ghana

ABSTRACT

This paper seeks to answer the question 'What factors determine bank employee reading habits of security policies? Using the chi-square test, this research analyses the reading habits of bank staff to ascertain whether there is significant difference in their reading habits with regards to the following independent variable- gender, the section of bank the employee works (whether department or branch), number of years the staff has worked with the bank and the ownership status of the bank (public, private or foreign owned). In addition, logistic regression was employed to determine the predictors of these reading habits. This paper adopts a quantitative research methodology to study the information security reading habits of 136 Ghanaian bank staff from various banks and concludes that bank staffs working in departments are more likely to regularly read their banks policies than employees working in a branch. This paper also shows that there is statistical significant difference in reading habits with regards to the number of years an employee has worked with the bank. The paper finally shows that there is no statistical significant difference in security reading habits with regards to gender and ownership status of the bank. The logistic regression analysis also reveals that a respondent in a department is 4.4 times more likely to read the security policies relative to those in a branch. The analysis also concludes that , respondents who have worked for less than 5 years were less likely to read the policy relative to those who have worked more than 5 years (OR=.51)

Keywords: Computer Security, Security Policies, User Attitudes

1. INTRODUCTION

Information Security plays a very crucial role in the protection of a bank's network systems. With the advent of the World Wide Web, e-commerce and e-banking and its attendant security risks such as cyber crime, the need to protect a banks's network and data becomes more relevant. Apart from providing technical solutions such as anti-virus software, firewall systems, intrusion detection system, cryptology, organizations also attempt to influence and manage the behaviour and activities of their employees through information security policies which spells out the do's and don'ts of the use of computer systems. Organizations also supplement the

Manuscript first received/*Recebido em:* 03/08/2013 Manuscript accepted/*Aprovado em*: 03/10/2014

Address for correspondence / Endereço para correspondência

Willian Allassani, University of Professional Studies, Department of Information Technology, Legon-Accra, Ghana. E-mail: wallass123@yahoo.com

effectiveness of these security policies and procedure by organizing regular training programmes for their employees.

A security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but continuously updated as technology and employee requirements change. An information security policy addresses many issues such as: disclosure, integrity, and availability concerns; who may access what type of information in what type of manner; basis on which the access decision is made (for example, user characteristics such as nationality or group affinity, or some external conditions such as time or status); maximized sharing versus least privilege;separation of duties; who controls and who owns the information; and authority issues, (Olson and Abrams 1995) The first stage of defining a security policy is to determine the security needs of a given community, express those needs in a formal requirement, followed by a description of how the company plans to educate its employees about the policies, (Goguen and Meseguer,1982). A company's security policy may include an acceptable user policy in the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

However, over the years, the activities of employees in the use of computers have tended to be counter-productive in the sense that it does not fall in line with the information security policies of their organizations. This stems from the fact that users sometimes adopt a negative attitude to these security policies and flout its directives. There is therefore the need to assess and investigate the attitude of users towards information security in general and information security policies in particular and why they sometimes flout these policies. According to Besnard and Arief (2004), computer security has traditionally been assessed from a technical point of view and that another way to assess it is by investigating the role played by legitimate users of systems in impairing the level of protection. They further argue that, from research in psychology, it is known that people make biased decisions and as a result sometimes overlook rules in order to gain maximum benefits for the cost of a given action. This situation leads to insidious security lapses whereby the level of protection is traded off against usability.

Ghana’s banking sector has improved by leaps and bounds, thanks to the introduction of technology. Universal banks operating in Ghana have introduced lots of technology-driven products and services which have led to massive growth in the sector. However, Ghana’s banking industry has not been spared the downside of technology. There have been reported cases of fraudulent practices by bank employees most of which involves the manipulation and misuse of computers systems. There is therefore the need for the banks to strengthen their computer protective systems starting from controlling the security behaviour of their employee, which can be done through sound and effective security policies and procedures. Computer security is important to all businesses particularly for banks, Checkley, (1994). According to O’Leary, Williams and O’leary (1989) two issues come to mind when banks talk about security. They are privacy and controlling whoever gets access to the bank’s computer systems and its programmes and what time to access them. They explain privacy as being primarily a personal concern; it is the assurance from the banks to individual banking customers that personal information will be used properly or accurately and protected from improper access either from within or outside the bank.

One of such a fraudulent activity as reported in the press involves the manipulation of a bank's computer system where false credit and debit balances were recorded to assist a branch manager grant unauthorised overdrafts. The false entries were described in various ways in the bank's books as transfers, sundry cheques, uncleared cheques, reversed cheques, cash, and telegraphic transfer. With the now infamous case of Kweku Adoboli, the thirty-one-year-old Ghanaian who was arrested in connection with the 2 billion dollar bank fraud at a Swiss Bank, UBS in London readily comes to mind. This led the bank to be fined £30 million by Britain's financial regulator for failures in its systems and controls that allowed Kweku Adoboli to conduct Britain's biggest bank fraud, Daily Telegraph (2012).

Considering the foregoing challenges within the Ghanaian banking sector among others, this study aims to examine the information security habits of bank employees with special emphasis on the reading habits of security policies and procedures. Employees can only exhibit good security behaviour if they know the do's and don'ts of the use of computer system, and these can only be known via information security policies and procedures.

2. RESEARCH BACKGROUND

Commercial banking started in Ghana in 1874 when Standard Chartered Bank, then known as Bank of British West Africa, opened a branch in Accra. They were closely followed by Barclays bank, which started its operations in Accra in 1917. It was not until 1953 when the first state owned bank, Bank of the Gold Coast, was established to be followed by the establishment of a central bank, Bank of Ghana, and the first indigenous commercial bank, Ghana Commercial Bank, in its independence in 1957. The formation of these two banks was the result of the splitting of the Bank of the Gold Cost.

A number of banks, mostly state-owned banks were subsequently established and in December 2001 there were 17 banks in Ghana, IMF (2007). They are Ghana Commercial bank, Barclays bank, Standard Chartered Bank, SG-SSB Bank, Bank for Africa (then Amalgamated Bank), Agricultural Development Bank, National Investment Bank, Merchant Bank, CAL Bank, Ecobank, First Atlantic Bank, Stanbic Bank, UT Bank (formerly Metropolitan and Allied Bank), Prudential Bank, Unibank, International Commercial Bank, The Trust Bank (now part of the Ecobank Group).
According to Bank of Ghana´s updated list of banks for 2012, there are 25 recognised universal and fully operational banks in Ghana with 882 branches. The ownership status of the banks is made up of 4 publicly owned banks, 14 foreign owned banks and 7 privately owned banks.

Table1: Universal Banks Operating in Ghana on 31 December 2012

Name of Bank	Year of Incorporation	Ownership Status	Number of Branches
Access Bank	2008	Foreign	31
Agricultural Development Bank	1965	Public	91
Bank for Africa	1997	Foreign	20
Bank of Baroda	2007	Foreign	1
Barclays Bank	1917	Foreign	92
Sahel Sahara BANK	2008	Foreign	11

Name of Bank (cont.)	Year of Incorporation	Ownership Status	Number of Branches
CAL Bank	1990	Private	18
Ecobank	1990	Foreign	78
Energy Bank	2010	Foreign	3
Fidelity Bank	2006	Private	31
First Atlantic Merchant Bank	1994	Private	7
Ghana Commercial Bank	1953	Public	157
GT Bank	2004	Foreign	22
HFC Bank	1990	Private	24
International Commercial Bank	1996	Foreign	17
Merchant Bank	1971	Public	22
National Investment Bank	1963	Public	27
Prudential Bank	1993	Private	32
SG-SSB Bank	1975	Foreign	45
Stanbic Bank	1999	Foreign	23
Standard Chartered Bank	1896	Foreign	35
UniBANK	1997	Private	19
United Bank for Africa	2004	Foreign	32
UT Bank	1995	Private	24
Zenith Bank	2005	Foreign	26

Source: Ghana Banking Survey 2012-PricewaterhouseCoopers (Ghana) Ltd

The main segments served by the Ghanaian banking sector are corporate and institutional, retail and SME entities. Entities that are served by the Ghana banking industry are mainly in the oil and gas, commerce, manufacturing and agricultural sectors. The Ghanaian banking industry over the last 3 years has had impressive records in terms of profitability, return to shareholders, deposit mobilisation, and operating assets. According to the 2012 Ghana Banking Survey, the industry profits before tax margin rose from 27% in 2010 to 30.6% in 2011. This was attributable to an 18% decline in interest expense and a 30% increase in net fees, commission income, compared to 2% decline and 18% increase in 2010 respectively. According to the report, industry profits after tax increased by 28% in 2011. The report further states that shareholder equity increased by GHc484 million in 2011 due to the combined effect of GHc280 million capital injection and GHc204 million in the form of statutory or reserves retained by bank reserves. Overall industry return on equity increased from 16.6% to 17.9%. The industry's operating assets grew from GHc16.4 billion in 2010 to Ghc19.9 billion in 2011. Loans and advances continued to be the most significant component of the industry´s earning assets as it contributed to approximately 63% of total income of banks despite the decline in the average lending rates, from 27.7% in December 2010 to 25.96 in December 2011. The Ghana Banking Survey showed that total industry deposits grew by 28% in 2011. It is significant to note that in both 2010 and 2011, more than 80% of deposit liabilities held by banks were non retail. The average base rate fell from 24.3% to 21.5% in 2011. Lending rates followed a similar trend and dropped from an average of 27.6% in January 2011 to 25.9% in December 2011.

With the above impressive performance by the Ghana banking sector over the last couple of years, it is expected that all efforts would be geared towards sustaining this performance. It is therefore imperative that banks put in place a mechanism that

blocks all loopholes that could lead to loss of revenue which could be perpetrated through manipulation of computer systems; hence the need for protecting banks' information technology infrastructure and system from inside and outside the bank.

Information Technology is a modern handling of information by electronic means which involves its access, storage, processing and transmission. Alu (2002) also asserts that information technology positively affects financial institutions by easing enquiry, saving time and improving service delivery. It is not surprising that Ghanaian banks have fully adopted Information Technology in their quest to provide e-banking products and services. Currently the 25 banks in Ghana offer various types of technology-driven products and services. They include networked branches, internet banking, telephone banking, mobile banking, card services, and Automated Teller Machines (ATM).

However, it must the noted it was not until foreign banks, especially from Nigeria entered the Ghanaian banking industry from 2004, that real e-banking took off. The earliest form of electronic banking in Ghana in the 1980's was the use of telex, telephone, and facsimile, Abor (2001). These gadgets were used for the exchange of information, and especially transfer of funds between branches of the same bank. Out-station cheques for clearing took a minimum of 28 working days to clear. Other banking operations such as cheques for payment over the counter, issuing of bank drafts, salaries of workers from both Government and private establishments were all processed manually

As competition in the banking industry intensified and computers begun to take the centre stage, banks like Ghana Commercial Bank, National Savings and Credit Bank (later became part of SG-SSB Bank) and Bank for Housing and Construction (later liquidated) started using computers in back office operations. The most significant development in the electronic banking in Ghana was the introduction of the Automatic Teller Machine (ATM) by The Trust Bank (now part of the Ecobank Group) in 1995. Ghana Commercial Bank also introduced their ATMs in 2001 in collaboration with Agricultural Development Bank, Abor (2001).

Another technological innovation in Ghanaian banking was the various electronic cards, which the banks have developed over the years. The first major card product was a cash card product of Social Security Bank, now S-G SSB, introduced in May 1997. Their card, 'Sika Card' was a value card, onto which a cash amount is electronically loaded. Standard Chartered Bank launched the first debit card in Ghana in 2001, Abor (2002). A consortium of three (3) banks (Ecobank, Cal Merchant Bank and The Trust Bank) introduced a further development in electronic cards in November 2001, with a product called 'E-Card'. This card was online in real time, so a client uses the card at anytime, or if changes occur in their account balance, their card automatically reflects the change.

Barclays Bank also launched its telephone banking services in 2002. SSB Bank also launched its "Sikatel" or "SSB Call Centre" (telephone banking) in 2002 (Abor 2001). The services available with this system were ascertaining information about the bank's products and services, customers' complaints, bank statements and cheque book request and any other complaints and inquiry.

Between 1995 and 2002 a lot happened in the Ghanaian banking sector in terms of technology adoption and the introduction of e-banking. However it was not until 2004 when internet banking, and other related e-banking products such as Card

Payment systems started permeating the banking industry. This was after Nigerian banks like United Bank for Africa (Formerly Standard Trust Bank) Guarantee Trust Bank (GT Bank) and Zenith Bank had entered the Ghanaian banking industry and fully rolled out these services. Today all the 25 universal banks have rolled out comprehensive e-banking products including internet banking, international debit and credit cards, mobile money payments, e-statements, sms banking, and many more.

Problem Statement

Banks in Ghana use different methods in ensuring that its employees are made aware of these policies and the implications for non adherence to the policies. In some banks, branches and departments keep copies of the policy document and employees are expected to read and attest they have read the policies. The attestation is repeated every six months. Attestation by an employee gives the banks the right to summarily dismiss an employee for any behaviour that leads to a security breach or incident. Kankanhalli et al (2003) define computer security incident among others as a violation of any computer security policy. Other banks also give copies of security policy documents to newly recruited staff to read during the period of orientation. Another method of dissemination of security policies within the banks is through the bank's intranet where employees are expected to read the policies online which are subsequently monitored through audit trail systems. Bank employees are expected to read policies regularly, at least every six months to update themselves on new development and other updates. According to Santon et al (2004) success in computer security depends on the effective behaviour and attitude of users. It pre-supposes that any untoward behaviour by users would spell disaster for organization.

What recent studies about the attitude of bank employees towards information security behaviour by users, especially in the banking industry, have not captured is whether there is a disparity in the attitude towards computer security in terms of gender, number of years worked with the bank, the section employees work (whether a branch or a department) and whether there is a disparity in terms of ownership status i.e. public, private, or foreign owned.

So the question is 'do bank employees in Ghana regularly read their banks´ security policies? What are bank employee reading habits of security policies and what determines and influence those habits? Extensive research carried out for empirical literature on information security in general and security policies, in particular within the Ghanaian business, or education sector in general and the banking sector in particular lead to no clear results. Thus, to the best of the author's knowledge no empirically tested literature is available on Information security policies within the banking sector of Ghana. It is therefore a very fertile and virgin area which researchers can look at. Most empirical research in security in Ghana relates to food and nutrition security, security of land tenure etc.

This paper therefore seeks to find out if bank employees in Ghana read their banks´ security policies and what factors influence their reading habits and what the differences are, if any, in the reading habits.

Hypothesis of the Study

The study is guided by the following hypotheses:

Ho: There is no statistically significant difference in the security policy reading habits between bank employees based in branches and employees based in departments.
Ho There is no statistically significant difference in the security policy reading habits between bank employees with regards to the number of years they have worked with the bank.
Ho: There is no statistical significant difference in the security policy reading habits of bank employees as far as gender is concerned.

3. LITERATURE REVIEW

The importance of Information security to the banking sector cannot be over-emphasised. Researchers and academics have undertaken a number of researches in the area of Information security and especially end-user behaviour and attitude to information security.

User Security Behaviour.

Organizations increasingly rely on information systems for processing, transmission and storage of information. Consequently, it is essential to protect the information within these systems and the availability of these computer systems. However, while deploying technological solutions and counter measures is important to avoid security risks, (Claburn, 2005), improving the level of security awareness of users is equally if not more important (Tim, et al 2004); (Vijayan, 2005).
D'Arcy et al (2009) contend that intentional insider misuse of information systems resources (i.e., IS misuse) represents a significant threat to organizations. For example, industry statistics suggest that between 50%–75% of security incidents originate from within an organization.

Thus, they suggest that there is the need to understand user security behaviour with a view to ensuring that those behaviours are in tandem with organization security policies. They developed an extended deterrence theory model that combines work from criminology, social psychology, and information systems. The model posits that user awareness of security countermeasures directly influences the perceived certainty and severity of organizational sanctions associated with information system misuse, which leads to reduced misuse intention. The model was tested on 269 computer users from eight different companies. The results suggest that three practices deter information systems misuse: (a) user awareness of security policies; (b) Security Education, Training, and Awareness (SETA) programs; (c) computer monitoring. The results also suggested that perceived severity of sanctions is more effective in reducing information system misuse than certainty of sanctions. Further, their research showed that the impact of sanction perceptions vary based on one's level of morality.

Empirical Research on Determinants of user Security Behaviour

While there is a rich body of literature on user acceptance of technologies with positive outcomes, there is little empirical research on the determinants of user security behaviour. Igbaria et al (2005) studied user behavioural intention toward protective technologies based on the framework of the theory of planned behaviours. They

defined information technologies as what protect data and systems from disturbances such as viruses, unauthorized access, disruptions, spyware. Their studies found out that awareness of the threats posed by negative technologies is a strong predictor of user behavioural intention toward the use of protective technologies. They also posited that, in the presence of awareness, the influence of subjective norm on individual behavioural intention is weaker among basic technology users but stronger among advanced technology users. Furthermore, while their results are consistent with many of the previously established relationships in the context of positive technologies, they also found out that the determinants 'perceived ease of use' and 'computer self-efficacy' are no longer significant in the context of protective technologies.

Ng, et al (2008) carried out studies that used the Health Belief Model (HBM) to study users' computer security attitude. They validated the HBM model using survey data from 134 employees. Results showed that perceived susceptibility, perceived benefits and self efficacy are determinants of e-mail related security behaviour when applied to exercising care with e-mail attachment. The HBM is one of the earliest comprehensive attempts to explain health care behaviour on expectancy value principles. (Rosenstock, 1974). However, the limitation of this research is that only one security practice was measured, i.e. e-mail security.

It must be noted that the work of Ng et al (2008) contradicts the work by Ibgaria, Guimaraes and Davis (2005) who concluded that computer self-efficacy is no longer significant in the context of protective technologies. However, the internet relies heavily on protective technologies such as anti-virus software, intrusion detection systems, etc.

Dinev, et al. (2008) developed a theoretical model of user behaviour based on the framework of the theory of planned behaviour and national cultural dimensions and indices. Using this model they carried out comparative studies across different cultures in which they examined the cross-cultural differences between South Korea and the United States in user behaviour towards protective information technologies. They concluded that cultural factors reduce the strength of the relationships in the behavioural model in the context of protective information technologies. The model was then empirically tested using structural equation modelling techniques in conjunction with multi-group analysis. Most of the hypothesized moderating effects of national cultural factors were found to be statistically significant. Their findings suggest that cultural factors should be considered in order to design effective information security policies, practices and technologies in global networks where multiple cultures coexist.

Dinev and Qing (2007) agree that the major threat to information security is constituted by careless employees who do not comply with organizations' information security policies and procedures. According to Dinev and Qing (2007) prior research on information security compliance has criticized these existing information security awareness approaches as lacking theoretically and empirically grounded principles to ensure that employees comply with security policies. To fill this gap, their study proposed a theoretical model that contains the factors that explain employees' information system security policy compliance. Data from 245 respondents from a Finnish company provided empirical support for the model. The results suggested that information quality has a significant effect on actual security policy compliance. Employees' attitude, normative beliefs and habits have significant effect on intention to comply with security policies. Their work also revealed that threat appraisal and facilitating conditions have a significant impact on attitude towards complying, while

coping appraisal does not have a significant effect on employees' attitude towards complying. They also concluded that sanctions have an insignificant effect on intention to comply with security policy and awards do not have a significant effect on actual compliance with IS security policy. The model did not, however, consider organizational attributes such as the ownership status of the companies (whether private, public) on the user compliance with security policies, neither did it consider the effects of demographics on users' compliance with security policies.

Determining the factors that influence general public acceptance of generic information technology solutions can be a daunting task. A lot of variables would have to be considered and this even makes the research more extensive. In their research, Hung, et al. (2006) identified the factors that determine public acceptance of e-Government services which was an online tax filing and payment system (OTFPS) in Taiwan. Using a theoretical model based on the theory of planned behaviour, this study had as its aims to identify the determinants for acceptance of the OTFPS and to examine the causal relationships among the variables of acceptance behaviour for the OTFPS, and to also explore the relative importance of each determinant for both those who use the OTFPS and those who do not. Based on a survey of 1,099 usable responses, the results indicated that the proposed model explained up to 72 percent of the variance in behavioural intention. In addition, the important determinants of user acceptance of the OTFPS are perceived usefulness, ease of use, perceived risk, trust, compatibility, external influences, interpersonal influence, self-efficacy, and facilitating condition.

Perceived security is defined as the level of security that users feel while they are shopping on e-commerce sites or using information technology systems. In their work, Yeniseya, et al. (2005) determined items that positively influence this feeling of security by users during shopping, and to develop guidelines for perceived security in e-commerce. A virtual shopping security questionnaire (VSSQ), consisting of fourteen perceived security items, was presented to the users. The VSSQ had a Cronbach's alpha internal reliability value of 0.70. With the exception of two items, they found no significant differences in item ratings between the groups of different shopping item values. A factor analysis procedure determined two main factors concerning perceived security in e-commerce. The perceived operational factor includes: the site's blocking of unauthorized access; emphasis on login name and password authentication; funding and budget spent on security; monitoring of user compliance with security procedures; integration of state-of-the-art systems; distribution of security items within the site; website's encryption strategy; and consolidation with network security vendors. The perceived policy-related factor includes: the website's emphasis on network security; top management commitment; effort to make users aware of security procedures; the website's keeping up-to-date with product standards; the website's emphasis on security in file transfers; and issues concerning the web browser.

The gap identified in the above literature has to do with the fact that most of the studies did not bring bio-data and organization characteristics to support their work. Another gap in the literature review has to do with little research on IT security within the banking and finance sector. Most research has concentrated on other sectors such as communication, educational institutions, manufacturing, military and government establishments. What's more, there has been lots of research on information security and user behaviour with emphasis on the developed world, but with little empirical research on the developing world. With the lack of theoretically grounded empirical

studies on whether users regularly read their organization's security policies and the lack of empirical studies on security behaviour within the banking sector and in the developing world, this study aims to find out information on bank employee reading habits of security policies in Ghana and what factors influence these habits.

4. METHODOLOGY

The study was conducted at the National Banking College in Accra. Founded in 1994, the National Banking College (NBC) was the first specialist academic training institution for middle to top level bankers. Over the years, the College has grown to carve a new mission and vision offering, from relevant applied research spanning a uniquely broad range of fields to specialist consultancy services. It is presently funded by the 25 universal banks and is under the supervision of the Bank of Ghana which also provides some funding for its operations. The college has 5 main faculties namely Banking Operations, Human Resource and Marketing, Information Technology, Treasury, Credit Operations, Corporate Reporting.

Data Gathering

A questionnaire was randomly distributed to 150 bankers from various banks who were attending various training programmes at the college. 136 of the questionnaires were returned made up of 82 male (60.3%) and 54 females (39.7) respondents. The questionnaire had three sections. Section one requested for information such as gender, number of years worked with the bank, and whether respondent worked in a department or branch. Section two requested for information on respondent's bank, its ownership status (whether public, private or foreign owned) the number of years the respondents bank has operated in the country. Section three requested for information on the bank's information security policies and procedure such as whether the respondent's bank has an information security policy in place, whether the respondent reads the policies, the number of times the respondent has read the policies, whether respondent's bank regularly monitors the security policy habits of employees. This section also wanted to know if respondents are more likely to read the policies, if senior executives are directly involved in the monitoring the reading habits of employees.

In all, 20 banks took part in the survey. They are made up of 19 banks out of the 25 universal banks in the country, and Bank of Ghana as indicated below.

Table 2 Banks that took part in the survey

Participating Banks	No of Respondents	Participating Banks	No of Respondents
Access Bank	4	HFC Bank	9
Agricultural Development Bank	3	International Commercial Bank	4
Bank for Africa	9	Merchant Bank	6
Bank of Ghana	7	National Investment Bank	6
Barclays Bank	4	Prudential Bank	8
CAL Bank	4	Sahel Sahara Bank	7
Ecobank	11	Standard Chartered Bank	4

Participating Banks (cont.)	**No of Respondents**	**Participating Banks**	**No of Respondents**
Fidelity Bank	7	Unibank	4
Ghana Commercial Bank	12	United Bank for Africa	11
Guarantee Trust Bank	10	Zenith Bank	6
Total			**136**

Data Analysis

Data was analysed using SPSS 18.0. Logistic regression was employed to examine factors that predict two outcomes; firstly, whether the bank employees read the policies or not, and secondly, whether they would read the policies if senior executives are involved in the monitoring of reading habits. This enabled the computation of the probability that a respondent reads or does not read the security policies using covariate

The study has two dependent variables: reading or not reading bank's security policies and whether executive involvement in monitoring reading habits would influence respondent to read or not. Independent variables in this paper are: gender, the number of years worked with the bank, the section of the bank where the respondent works (department or branch), and ownership status of the bank (whether public, private and foreign owned). The study sought to find out if these variables have any effect on the reading habits of respondents.

The analysis of the determinants of each of the two dependent variables was done separately. Both bivariate and multivariate analysis were performed to explore the determinants of reading or not reading bank's security policies as required by bank rules, and reading the policies if executives is involved in monitoring reading behaviour. The statistical significance was based on a p-value of less than 0.05.

5. RESULTS

Bivariate Analysis of Respondents who Read or Do not their Bank's Security Policies.

Of the 136 respondents a total of 71 representing 52% of respondents said they read their bank's policies against 65 representing 48% of respondents who do not read their banks policies.

In this section, the paper explores at the bivariate level, the differences between those who read the policies as stipulated by the banks´ regulations and those who do not read them, and thus flout their banks' regulation. As seen in Table 3, there was a significant difference ($p < 0.0001$) between those who work in departments and those based in branches with regards to those who read and those who do not read security policies. In terms of the number of years, a respondent who has worked in the bank, there was a slight significance ($p < .010$) between those who have worked for less than 5 years, those who have worked for more than 5 years, but less than 10 years and those who have worked for more than 10 years. There was however no significant difference in terms of gender ($p = .209$) and the ownership status of the banks ($p = .781$)

Bivariate Analysis of Respondents who would read policies if Senior Executive are involved in the monitoring of reading habits

118 respondents representing 87% said they would read the policies if bank executives are involved in the monitoring of employees reading habits, while 17 respondents representing 13% said they would not read them. From Table 3, it can be seen that there is no statistical significance differences in terms of gender (p = .531), section of the bank that respondent works (p = .314), ownership status of bank (p = .983) and length of service of respondents (p = .910)

Table 3 - Bivariate Analysis of respondents who read security policies and those who would read if senior executives are involved in monitoring reading behaviours

Characteristics	% of Respondents who have read or have not read policies		P-value	% of respondents who will read policies if executive is involved		P-value
	Yes	No		Yes	No	
Gender						
Male	48.8	51.2		87.8	12.2	
Female	57.4	42.6	**.209**	86.8	13.2	**.531**
Section of the Bank where the respondent Works						
Department	67.6	32.4		89.6	10.4	
Branch	36.8	63.2	**.000***	85.3	14.7	**.314**
Ownership Status of Banks						
Public	52.9	47.1		88.2	11.8	
Private	46.9	53.1		87.5	12.5	
Foreign	54.3	45.7	**.781**	87	13	**.983**
Length of Service						
5 yrs or less	43.1	56.9		86.2	13.8	
More than 5 yrs but Less than 10 years	54.5	45.5		88.9 87	11.1	
More than 10 years	69.6	30.4	**.090****		13	**.910**
Total	**53.19**	**46.81**		**87.4**	**12.57**	

* Statistically Significant at 1%
** Statistically Significant at 10%

Multivariate Analysis

Separate analysis were undertaken for each of the two outcomes variables: reading the banks policies in compliance with bank's rules, and reading policies provided executives are involved in monitoring employee reading habit. To evaluate possible impact on each of the two outcome variables by personal level and bank attribute variables, multivariate logistic regressions were employed. The results are presented in Table 4 and it shows a statistical significance for the relationship between the two variables and the explanatory variables considered in this paper.

One of the major objectives of this study is to identify key variables that strongly explain the security policy reading habit of respondents. Two predictors were identified, i.e. the section where a respondents works (department or branch) and the number of years a respondent has worked in the bank. A respondent who worked in a department is 4.4 times more likely to read the policies than a respondent who worked in a branch (OR = 4.446, p = .000). The number of years a respondent has worked with the bank was found to be a weak predictor of reading habits (OR = .507, P = .016). The study however showed that gender and ownership status of a bank are not predictors of security policy reading behaviour of respondents: (Gender: OR=.602, p = .202) (Ownership Status of Bank: OR= .742, p=.208).

The studies revealed that all the four covariates are not strong predictors of the second outcome, i.e. whether respondents would read policies if senior executives are involved in the monitoring of reading behaviour of employees**.**

Table 4 - Multivariate analysis of determinants of banks´ security policy reading habits and banks´ security policy reading habits if executives are involved in monitoring reading habits

Variables	**Analysis of Reading Policies as a rule**		**Analysis of reading policies if reading habits are monitored by senior executives**	
	OR	**Sig**	**OR**	**Sig**
Gender	.602	.202	1.072	.899
Number of years Worked with Bank	.507	.016*	.922	.831
Section of Bank respondent works	4.446	<.000*	1.466	.473
Ownership status of bank	.742	.208	1.035	.918

Statistically significant difference at $p < 0.05$

6. DISCUSSION

This survey showed that almost half of respondents, i.e., 47% do not read their bank's security policies and procedures. The study also revealed that whether a respondent reads the policies or not greatly depended on one very important explanatory variable, that is, the section of the bank where the respondent works. Respondents who work in departments are more than 4 times likely to read the security

policies than respondents who work in branches. This may be as a result of the fact that employees in branches are the "face of the bank" because they deal directly with customers of the bank all the time and may not find the time to read the policies. Unlike employees based in branches, employees based in departments may not necessarily deal directly with customers. If employees in departments deal directly with customers at all, the numbers would not be as the number of customers employees in branches have to contend with.

The study also showed that the 87% of the respondents would read the bank's policies if senior executives are involved in the monitoring of security policy behaviour. The key predictor for this outcome is the number of years the respondent has worked with the bank. Respondents who have worked for less than 5 years in the bank are .51 less likely to read the policies than those who have worked in the bank for more than 5 years. This could stem from the fact that the longer an employee stays with the bank, the more conversant he/she becomes in terms of the culture of the bank, the more likely he/she practices that culture. Another possible explanation for this phenomenon is that the longer an employee has worked with the bank, the more likely he would have experienced some sanctions with regards to non-compliance with security issues.

Finally this study shows that there is no statistically significant difference as far as gender and ownership status of banks are concerned ($p = .209$). There is also no statistically significant difference with regards to reading habits as far as ownership status of banks is concerned ($p = .781$). Irrespective of whether a bank is public, private or foreign, it has no bearing on the security policy reading habits of its employers.

7. CONCLUSION AND RECOMMENDATION

This study has produced important information on bank employee reading habits of security policies. It has been established through this study that the main predictor of bank employees' security policy reading habits is the section of the bank that the employee works. Employees based in branches are less likely to read security policies due to the fact that they deal with a huge number of customers each day and thus have little time to read these policies. The study also finds that there is a strong link between reading the policies and the number of years an employee has worked with the bank. Employees who have worked less than 5 years are less likely to read even if senior executives are involved in the monitoring process.

Based on these findings this study wishes to recommend that banks create reward systems to all employees who show good reading habits as far as reading security policies are concerned. To also encourage employees to read the policy, banks should make reading of the policies part of end-of year appraisal and tied to end of year bonuses. Banks should also make it financially attractive for employees who work in branches to come to work on weekends purposely to read the banks security policies and procedures.

These findings should not be seen as a local issue pertaining to Ghana, but that it is likely that such reading habits can be found within banks on the African continent. This is because most of the banks operating in Ghana have their parent companies located in other African countries, notably Nigeria and South Africa. What's more,

these banks move staff around the continent and it is likely that there could be a transfer of attitudes around the continent

8. LIMITATIONS OF RESEARCH

The first limitation of this study is the sample size. Due to the difficulty getting responses from bank employees when they are on the job in their banks, this study targeted a small number of bank employees who were attending training courses at a central location and were, therefore, more receptive to giving responses to survey questionnaires. It is recommended that this study is carried out with a much larger sample size and more independent variables such as age, education qualifications, and marital status.

The second limitation is the level of staff involved in the survey. All the respondents were senior staff of the banks. Further research should be carried out to include junior staff, by comparing the reading behaviour of senior and junior staff.

REFERENCES

Abor, B (2001) Technological Innovations and Banking in Ghana: An Evaluation of Customers' Perceptions. http://www.financialanalyst.org/Technological%20Innovations%20and%20Banking%20in%20Ghana%20-%20AAFM.doc. Retrieved 24 June, 2012.

Alu A.O, (2000) Effects of Information Technology on Customers Service in the Banking Industry in Nigeria. Information Technology Review. 3(1), 5-19.

Besnard, D., & Arief, B. (2004). Computer Security Impaired by legitimate users. Computers & Security, 23(3), 253-264.

Boon-Yun N, Kankanhalli A, Xu Y, C (2009) Studying Users Computer Security Behaviour: A health Belief Perspective Decision Supports Systems, 46, 815-825.

Checkly J, (1994) Electronic Banking Security: Banking System Security. Brain Welch (ed) P47. Basel Blackwell

Claburn, T. (2005, 2007). Spam cost billions. http://www.informationweek.com/story/showArti cle.jhtml?articleID=59300834. Retrieved 24 June, 2013

D'Arcy J, Hovav A, Galletta D. (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information System Research, 20(1), 79-98.

Daily Telegraph (2012) UBS fined £30m over Kweku Adoboli fraud failures. http://www.telegraph.co.uk/finance/financial-crime/9702513/UBS-fined-30m-over-Kweku-Adoboli-fraud-failures.html Retrieved 24 June 2012

Dinev T , Qing Hu (2007) "The Centrality of Awareness in the Formation of User Behavioural Intention toward Protective Information Technologies," Journal of the Association for Information Systems, 8(7), Article 23.

Dinev T, GooJ, Hu Q, Nam K (2008) User behaviour towards protective information technologies: the role of national cultural differences. Information Systems Journal, 19(4) 391–412.

Goguen, J. A., & Meseguer, J. (1982, April). Security Policies and Security Models. In IEEE Symposium on Security and privacy (Vol. 12) http://scholar.google.com/scholar?cluster=16438665001756746046&hl=en&as_sdt=0, 5# Retrieved on 24 June 2013.

Hung S, Y, Chang C,M , Yu T,J (2006) Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. Government Information Quarterly, 23(1), 97–122.

Ibgaria M, Guimaraes T, Davis G, B (1995) Testing the determinants of Microcomputer Usage via a Structural Equation Model. Journal of Management Information Systems - Special section, 11(4), 87 – 114.

IMF (2007) Staff Country Report. Capital Markets P.25

Kankanhalli A, Teo H.H, Tan B.C.Y, Wei K.K (2003) An integrative study of information system security effectiveness, International Journal of Information Management 23

O'Leary T.J. Williams B.K, O'Leary L. (1989). McGraw Hill Microcomputing. Annual Edition McGraw Hill

Olson, I. M., & Abrams, M. D. (1995). Information security policy. Information Security–and Integrated Collection of Essays. http://www.acsac.org/secshelf/book001/07.pdf Retrieved on 24 June 2013.

Park, C. H., & Kim, Y. G. (2003). Identifying key factors affecting consumer purchase behavior in an online shopping context. International Journal of Retail & Distribution Management, 31(1), 16-29.

Rosenstock I.M (1974) The health belief model and preventive behaviour. Health education monographs

Santon J.M, Mastrangelo P.R, Stam K.R, Jolton J (2004).Behavioral Information Security:Two end-user survey studies of innovation and security practice, Proceedings of the Tenth America's Conference on Information Systems, New York.

Stanton J.M, Stama K,R, Mas**tra**ngelo P, Jolton J (2005) Analysis of end user security behaviours. Computers & Security, 24(2), 124–133.

Timms, S., Porter C, Bead A (2004) Information System Security breaches Survey. UK Department of Trade and Industry Survey Report.

Vijayan J (2005) Targeting the enemy within. Computer World, 39(32), 23-26.

Yeniseya M.M, Ozokb A.A, Salvendycd (2005) Security Determinants in e-commerce among Turkish university students . Behaviour & Information Technology, 24(4), 259-274.

Yi-Shun Wang, Yu-Min Wang, Hsin-Hui Lin, Tzung-I Tang, (2003) Determinants of user acceptance of Internet banking: an empirical study, Emerald 14.