Internet Banking Security Concerns: An Exploratory Study of Customer Behaviours based on Health Belief Model

Bright Kwame Ameme, Ezer Osei Yeboah-Boateng

Abstract*—Internet banking is becoming increasingly important to banks in providing convenient banking services to customers. To attract and retain their customers, banks ensure security measures are put in place to protect the customers from various cyber attacks. Despite these security measures, customers are constantly being exposed to fraud and security issues. This paper therefore seeks to understand the reasons behind these security breaches and to develop a model to predict the behaviours of internet banking customers. Drawing on Health Belief Model, this paper employed chi-square and logistic regression analysis to specifically investigate internet banking security issues from human behavioural perspective. The study empirically revealed that there is a direct relationship between internet banking security breaches and customer behaviours. A predictive model was however developed to predict these human behaviours on internet banking platforms. The study concluded that internet banking security breaches are mainly due to human behaviours such as unlocking computers when not in use, installation of softwares from sources that are not trusted and supported, poor password management, and other related behaviours that could be prevented by customers. It was also concluded that there is no relationship between customers' age group and internet banking security breaches. It is therefore by chance that the younger respondents experience internet banking security issues more than the elderly. This chance could be attributed to the fact that the younger ones do not have valuable cash deposits to protect and hence not cautious in their behaviours on internet banking platforms. The findings of this study have important policy implications for banks, thereby helping to understanding the behaviour of customers on internet banking platforms. It is therefore recommended for banks to educate and organise regular and continuous security awareness programmes for their customers.

***Index Terms*— Internet Banking, Behaviours, Security.**

I. INTRODUCTION

Today, the banking sector is being driven by information and communication Technology (ICT). Banks are currently using information and communication technologies to offer products and services to their customers. An example of such technologies is the internet banking technology used to electronically offer banking services to customers. Whilst these technologies are essentially employed to provide convenience to customers, they also expose the customers to theft, fraud and other security related issues. Some of these security issues may be attributed to the behaviour of customers on these electronic banking platforms. According to [1], while technological advancements, evolving computer data systems, and internet access offer significant benefits to businesses and their customers, a major challenge that comes with the increased use of technology is an increase in the risk of cyber crime. Banks therefore need to focus on security when designing online banking systems. [2], states that "the banking field is the most exposed to security attacks and the financial losses are significant when security vulnerabilities are found and exploited". According to [3], Ghana has been identified as a major hub for cybercrimes within the West African sub-region. Ghana has also been ranked among the top 10 cybercrime offending nations in the world [4]. Despite the controls being put in place by banks in the design of online banking services, banks still record a number of internet banking security complaints which are mainly attributed to customers' behaviours over the internet. For example, internet banking users may knowingly or unknowingly share their internet banking login credentials with unathorised users. This and other unsecured customer behaviours could result in a compromise of an internet banking account and hence lead to a security breach that could negatively affect the customer.

A. Banking in Ghana

The banking sector plays a significant role in the Ghanaian economy. It represents the largest sector within the financial industry in Ghana. There are currently 30 banks operating in Ghana [5]. Banking in Ghana has been very competitive. These competitions are mainly driven by innovative and technological products and services. This was revealed by a study conducted by [6], one of the largest professional services firms in Ghana. The study revealed that bankers consider that technological factors will have the greatest influence on the future business of banking (p.10). Most banks in Ghana are offering internet banking services with basic self-service features such as bank account balance verification, generating bank account statement and fund transfers between accounts within the same bank. Some banks have Automated Clearing House (ACH) functionality which allows for transfer of funds between two banks (domestic transfers) through an intermediary, Ghana Interbank Payment and Settlement Systems (GhIPSS). Currently the domestic fund transfers are not executed in real time. To eliminate this deficiency, GhIPSS has introduced an instant bank transfer system known as the GhIPSS Instant Pay (GIP) which is expected to drive Ghana's economy closer to a cashless society.

Revised Version Manuscript Received on February 04, 2016.

Bright Kwame Ameme, Department of Information Technology, Ghana Technology University College, Accra, Ghana.

Ezer Osei Yeboah-Boateng, Ph.D, Faculty of Informatics, Ghana Technology University College, Accra, Ghana.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

B. Internet Banking in Ghana

Internet banking is simply considered as a system by which individuals, businesses or customers have access to their accounts, transact or transfer money, pay bills, obtain information regarding bank accounts and avail other banking related services through internet [7].Basic internet banking is defined as the three core internet banking services: balance enquiry, funds transfer and bill payment [8].[9] on the other hand defined internet banking or online banking as an internet portal used by customers for different kinds of banking services ranging from bill payment to investments (p.224). In this study, internet banking is defined as the provision of traditional banking services over the internet. As a result of customer demands and competition, banks in Ghana are expanding their service delivery channels by integrating them with other innovative services. An example is the integration of payment systems with internet banking platforms. This is to enable customers make payments for fees and utility bills. More than 70% of banks in Ghana are currently offering internet banking services to their customers. This significant number has revealed the high rate at which internet banking is penetrating the Ghanaian economy.

II. PROBLEM STATEMENT

Whilst the intention of banks in the introduction of alternate channels of banking is to improve efficiency and provide convenience to customers, these electronic channels tend to expose both banks and customers to some security risks. An example of such electronic channel of banking is the internet banking for performing banking transactions over the internet. So long as these banking interactions and transactions are performed over the internet, they are susceptible to security challenges. Whilst some of these security challenges can be addressed by the banks through the implementation of robust and secured systems, others can only be controlled by customers through their own actions and inactions. Inappropriate customer behaviour over the internet may expose customers to security and privacy abuses such as hacking, phishing, identity theft and other exploitations through the internet. It is against this background that this study was conducted to investigate customer behavioural issues that could impact internet banking security, with specific emphasis to Ghana.

III. OBJECTIVES OF THE STUDY

The main aim of the study is to explore customer behavioural issues that are likely to impact internet banking security. The study specifically seeks to achieve the following objectives;

1) To investigate the association between customer behaviour and internet banking security breaches.
2) To investigate the relationship between respondents' age group and internet banking security breaches.
3) To determine the extent to which various factors could help predict customer behaviour towards internet banking.

IV. RESEARCH QUESTIONS

The study therefore seeks to answer the following research questions;

1. What is the association between customer behaviour and internet banking security breaches?
2. What is the relationship between respondents' age and internet banking security breaches?
3. To what extent can the various constructs of the research model predict customers' behaviour towards internet banking?

V. SIGNIFICANCE OF THE STUDY

With the current rate of cyber crime in banking industry, it is essential to understand various threats and vulnerabilities within internet banking platforms and to propose measures that help to protect customers from these attacks. In other words, accessing banking services through the internet, exposes the banks and their customers to various security issues and hence the need to investigate how customer behavioural issues could impact on internet banking security. The significance of this study is mainly to address the information security concerns involved in the use of internet banking. This study is expected to provide education to customers and give better understanding of behaviours for preventing cyber attacks. The study is also expected to provide directions for implementing appropriate strategies that will improve customer confidence and trust in the use of internet banking services. In other words, the findings of the study will be relevant to banks as well as customers in protecting themselves from cyber crime and attacks.

VI. LITERATURE REVIEW

Several researches in the area of internet banking focus on factors affecting internet banking adoption and internet banking security from systems' perspective. In other words, most literatures on security fail to study customer behavioural issues that could impact internet banking security. A major reason for using internet banking service is the convenience it offers to users, where services can be accessed at anywhere and at any time. This was revealed by a number of studies - [10];[11];[12]. Despite this convenience, some customers are still skeptical about the use of internet banking services mainly due to security concerns. Some of these security concerns are system related whilst others are due to human behaviours. According to [13], "while technological controls are necessary, computer security also depends on individual's security behavior" (p.1). A study indicated that an individual learns to favour behaviours believed to have desirable consequences and not to favor those with undesirable consequences [14]. This study further revealed that if an individual perceives that benefits are derived from compliance or disadvantage from non-compliance, or that less effort is expended for compliance, a favourable attitude toward compliance is formed. A related study conducted by [15] states that "large number of information security breaches at the workplace result from employees' failure to comply with organizational information security guidelines" (p.1).This is supported by [16] stating that "the key focus of the behavioural IS security research has been on an organizational context" (p.4). This suggests the need to close this gap in literature by investigating security from human behavioural perspectives. This study is theoretically grounded on the Health Belief System, in which systems' vulnerabilities and related user behaviours are investigated using a model

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

originally developed to investigate individuals' behaviour within the health sector. This model investigated individuals' behaviour towards vulnerability to a serious health problem. The Health Belief Model (HBM), a psychological model originally developed in 1950 has become one of the widely used frameworks for investigating individuals' health behaviours. According to [17], the Health Belief Model (HBM) hypothesises that health-related action depends upon the simultaneous occurrence of three classes of factors:

1) The existence of sufficient motivation (or health concern) to make health issues salient or relevant.
2) The belief that one is susceptible (vulnerable) to a serious health problem. This is often termed perceived threat.
3) The belief that following a particular health recommendation would be beneficial in reducing the perceived threat, and at a subjectively-acceptable cost.

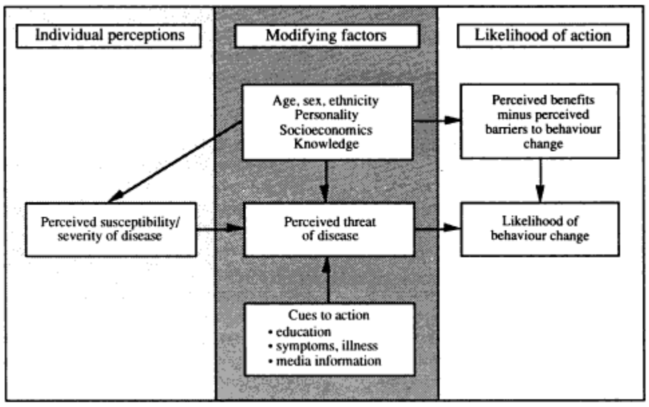


Fig. 1. The Health Belief Model [18]

Fig.1 shows the Health Belief Model. According to Rosenstock, Strecher and Becker (1988), the Health Belief Model has generated more research than any other theoretical approach, in the history of attempts to explain, predict, and influence health-related behavior (p.1). These researchers explained the framework by stating that for a woman (PERSON) to quit smoking (BEHAVIOR) for health reasons (OUTCOME), she must believe both that cessation will benefit her health (OUTCOME EXPECTATION) and also that she is capable of quitting (EFFICACY EXPECTATION), p.178. This study is conceptualised and applied to customer behaviours impacting internet banking security.

A. Research Model

The research model is bases on the Health Belief Model (HBM) as it focuses on measures capable of protecting individuals from harm.

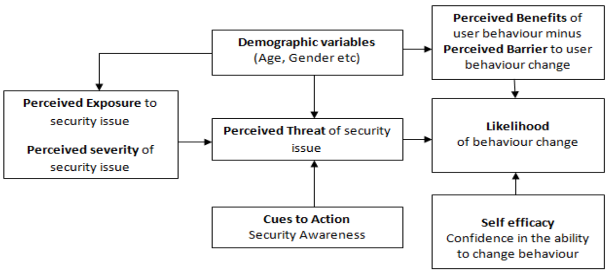

Demographic variables
(Age, Gender etc)
Perceived Benefits of user behaviour minus Perceived Barrier to user behaviour change
Perceived Exposure to security issue
Perceived severity of security issue
Perceived Threat of security issue
Likelihood of behaviour change
Cues to Action
Security Awareness
Self efficacy
Confidence in the ability to change behaviour

Fig. 2. Research Model

B. Types of Internet Banking

There are basically three types of internet banking services [19]. These are;

1) Informational: These are mainly marketing information about products and services.
2) Communicative: This type allows some interaction between a bank's system and the customers. These interactions include electronic mail exchanges, account balance enquiries and static file updates such as change of name and addresses.
3) Transactional: This type allows customers to perform financial transactions, e.g. electronic funds transfers and bill payments.

Each of these internet banking types have specific levels of risks associated with them. For example, the transactional types of internet banking services are highly risky and hence the need for customers to choose strong passwords for their internet banking transactions.

C. Customer Behaviours on Internet Banking Platforms

Whilst various social engineering techniques are employed by cyber attackers to gain unathorised access to user account information, the success or the failure of the technique largely depends on the end-users. For example, unauthorised access to internet banking platforms can be achieved through deceit and threats such as opening of unsolicited e-mails. This can compromise the security of users' personal computers which may have an impact on internet banking security. End-users may reduce their risk exposures through these behaviours;

1) Regular Update of operating system: This is done to maintain up-to-date operating system security patches on personal computers.
2) Updating browser software: Internet banking browser softwares are potential sources of vulnerabilities exploited by cyber attackers. Users are prone to security treats if their licensed internet banking browser softwares are not regularly updated.
3) Downloading free software: Internet banking users are prone to security breaches when they download from unsecured websites.
4) Checking for Malwares: These are malicious softwares intentionally included in a computing facility to cause harm to systems. Non-regular update of threat mitigation tools such as antivirus softwares leads to security breaches.
5) Password management: Intrusion prevention is the basic level of security which requires user authentication [20]. Good password management such as choosing strong and difficult-to-guess passwords for internet banking transactions helps to avert unathorised access.
6) Giving out real personal information: This refers to the users unintentionally giving out their personal information such as login credentials. This may be as a result of end-users falling foul of a social engineering technique.

VII. METHODOLOGY

This section describes the methods used in achieving the research objectives. It also explains the research design, data sources and collection method, the study population, sample size, sampling technique and the analysis of data.

A. *Research Design*

The study is a descriptive and cross-sectional study that is aimed at investigating customer behavioural issues that could impact internet banking security. This is a cross-sectional study as it focuses on a specific phenomenon at one specific point in time. Interviews and structured questionnaires were used as the data collection instruments. The research objectives were addressed using both quantitative and qualitative research methods.

B. *Population and Sampling*

The study population comprises all internet banking customers of banks in Ghana. Thirty (30) internet banking customers of a commercially licensed bank in Ghana were selected for the study. The respondents were selected from Accra, the capital city of Ghana. This is because the selected bank has majority of its branch networks in Accra, where most of the internet banking customers can easily be located. A stratified random sampling technique was employed to select 6 respondents from 5 chosen branches, evenly spread within the city of Accra.

C. *Data Collection*

The instrument used for data collection consisted of both closed-ended and open-ended questions. The closed-ended questions were made up of five-point Likert scale questions. The questions were thoughtfully designed to enable the researcher answer the research questions. Some interviews were also conducted to understand the feelings and lived experiences of customers in relation to internet banking security issues.

D. *Analysis of Data*

The study employed descriptive statistics such as frequency distributions to quantitatively analyse and summarise the data collected. Some speeches from selected respondents were also presented to share individuals' feelings and experiences on security issues encountered in the use of internet banking services. The quantitative analysis was done using statistical package for social sciences (SPSS). The following data analysis techniques were employed;

1) Cross-tabulations to investigate the association between customer behaviour and internet banking security breaches.
2) Cross-tabulations to investigate the relationship between customers' age group and internet banking security breaches.
3. Regression analysis to determine the extent to which various factors could predict customer behaviour towards internet banking.

VIII. RESULTS AND DISCUSSION

The main purpose of this section is to present the analysis and discuss the results of the study.

A. *Reliability Analysis*

Reliability and validity tests are essential in verifying the relationships between interrelated items or variables. The reliability of the variables was tested using Cronbach's alpha. Cronbach's alpha depends on the correlation between the variables. A higher degree of correlations represented by a higher value of alpha, is an indication of the internal consistency of the constructs under consideration.

Table: I Reliability of measurement variables

Variables	Number of items	Cronbach's alpha (>0.7)
Security Awareness	6	0.95
Severity and Exposure to Security Threat	4	0.89
Perceived Benefits of User behaviour	4	0.85
User Behaviour	11	0.96
User Behavioural Ability (Self-Efficacy)	3	0.87

The suggested alpha value should be greater than 0.7 for the measurement items to be considered reliable [21];[22]. In this study, User Behaviour displayed the highest internal reliability (alpha = 0.96) and Perceived Benefits of User Behaviour had the lowest alpha value of 0.85, as shown in Table I. Cranach's alpha coefficients indicated that all the variables had good reliability, as they had alpha values greater than the acceptable value of 0.7. Consequently, all the measurement variables were retained in the study

B. *Descriptive Statistics for Respondents*

The data collected include variables such as gender, age segment and educational level, in addition to other non-demographic variables used in answering the research questions. Out of a total of 35 administered questionnaires, only 30 responses were received.

Table: II Profile of respondents

Variables	N=30	Percentage
Gender	Male	63.30%
	Female	36.70%
Age Group	Less than 20	0.00%
	20-29	23.30%
	30-39	53.30%
	40-49	20.00%
	50 or more	3.30%
Level of Education	Professional certificate	10.00%
	Diploma	10.00%
	Bachelors Degree	43.30%
	Masters Degree	36.70%
	Terminal Degree	0.00%
Years of use of Internet Banking	Less than 1 year	20.00%
	1-3 years	26.70%
	More than 3 years	53.30%
Trained in Security Awareness	Yes	56.70%
	No	43.30%
Trust in Internet Banking	Yes	66.70%
	No	33.30%

Table II presents a summary of the relevant descriptive statistics of the respondents. The data collected also revealed that, out of the 30 respondents, 13 representing 45.2% behaved in ways that could result in compromising their internet banking user account details. No wonder, in response to a question about the use of different passwords across different websites, one interviewee had this to say:

Simply because I do not want to forget my passwords, I use same password for different applications and on different platforms, unless the password policy on a particular platform forces me to use a different password.

Also, 9 representing 30% of the respondents were at a point in time, affected by internet banking security issues. The high percentage of respondents (70%) who were not affected by any security issues on internet banking platforms shows that most users behave in a way that is likely to avert such security issues. This could be attributed to the relatively high percentage of respondents with security awareness training experience.

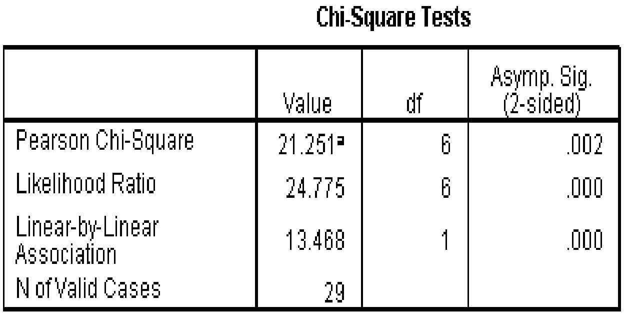
A chi-square analysis was conducted at 5% significance level (0.025 as a result of a 2-tailed test) and 6 degrees of freedom, to determine the relationship between customer behaviour and internet banking security experience.

Table: III Internet Banking Security Behaviour

		Good Internet Banking Security Behaviour				
		Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total
Experience of Internet Banking Security Issue	Sometimes	3	0	0	0	3
	Rarely	5	1	0	0	6
	Never	1	6	7	6	20
Total		9	7	7	6	29

The hypotheses tested are as follows;
H_0: There is no association between customer behaviour and internet banking security breaches.
H_1: There is an association between customer behaviour and internet banking security breaches.

Table: IV Chi-Square Test Results for Behaviour and Internet Banking Security Breaches



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.251ª	6	.002
Likelihood Ratio	24.775	6	.000
Linear-by-Linear Association	13.468	1	.000
N of Valid Cases	29		

There was a missing data resulting in number of valid cases of 29.The observed chi-square value was 21.251 as per Table IV. The critical chi-square value (χ0.025, 8) was however 17.535. Since the observed chi-square value of 21.251 exceeds the critical chi-square value of 17.535, the null hypothesis was rejected. This suggests that there is a relationship between customer behaviour and internet banking security experience. It is therefore not by chance that certain user behaviours leads to the experience of internet banking security issues. This finding is in line with [23], which reported that users change their behaviours because of security concerns. As one interviewee stated:

I always get scared whenever I hear of people complaining of security lapses in electronic banking products. Though I have internet banking access, I do not fully trust that it is safe and so I decided not to use it at all.

Table: V Age group of respondents

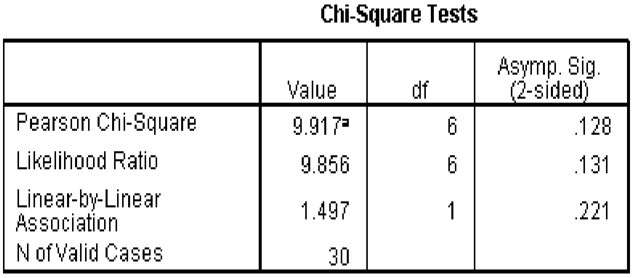
		Age Group				
		20-29	30-39	40-49	50 or more	Total
Experience of Internet Banking Security Issue	Sometimes	2	1	0	0	3
	Rarely	2	1	3	0	6
	Never	3	14	3	1	21
Total		7	16	6	1	30

Table V shows that 9 representing 30% of the respondents experienced internet banking issues and no respondent above 50 years experienced any internet banking issue. To ascertain whether or not the elderly with age group of 50 and above, are more security-conscious in their behaviour on internet banking platforms than the younger ones, a chi-square test was conducted to investigate the relationship between respondents' age group and internet banking security breaches. The hypotheses tested are as follows;

H_0: There is no relationship between customers' age group and internet banking security breaches.

H_1: There is a relationship between customers' age group and internet banking security breaches.

Table: VI Chi-Square Test Results for Age group and Internet banking security Issue



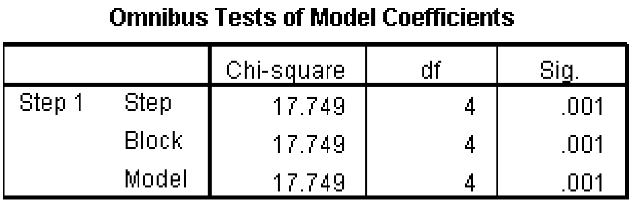
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.917ª	6	.128
Likelihood Ratio	9.856	6	.131
Linear-by-Linear Association	1.497	1	.221
N of Valid Cases	30		

At 5% significance level and 6 degrees of freedom, the observed chi-square value was 9.917 as per Table VI, whilst the critical chi square value was 14.449. Since the observed chi-square value of 9.917 was less than the critical chi-square value of 14.449, the researcher failed to reject the null hypothesis. This suggests that there is no relationship between customers' age group and internet banking security breach. It can therefore be concluded that it is by chance that the young respondents experience internet banking breaches than the elderly. As a result, the demographic variable (Age group) was excluded from the behaviour predictive variables used in the study.

In an attempt to determine the extent to which various variables of the research model could predict customer behaviour towards internet banking, a regression analysis was employed. The independent variables include threats/severity to security issues, security awareness, benefits derived from behavioural change and the confidence/ability to change behaviour (self-efficacy). The dependent variable is the likelihood of behaviour change. From the test results, if there are no predictive variables available for the researcher to make a prediction regarding customers' behaviour towards internet banking, 16 out of the 27 will not behave appropriately. Thus, the overall predictive ability of the model is 59.3% correct. In other words, without any predictive variable involved in the model, the researcher will correctly predict customers' internet banking behaviour around 59.3% of the time. The results revealed that the confidence/ability to change behaviour (self-efficacy) have a good predictive ability for customers' internet banking behaviour than the other predictor variables. However, the overall statistics has a significance level of 0.01 which is less than 0.05 and hence the model has a good predictive ability. This is confirmed by results from the Omnibus Tests of Model Coefficients.

Table: VII Results of Omnibus Test of Model Coefficients



Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	17.749	4	.001
	Block	17.749	4	.001
	Model	17.749	4	.001

From Table VII, the significance level is 0.01 which is less than 0.05. This indicates a significance model in which the predictor variables will do a good job of making a good or bad internet banking security behaviour prediction. The goodness of the model is also supported by Hosmer and Lemeshow's test results with a p-value of 0.770 which is expected to be greater than 0.05 for a model to be considered statistically significant. Nagelkerke R-Square from the test results was 0.650 indicating that 65% of the variance is explained by the predictors and this is decent.

Table: VIII Regression Logistic Test Results

	B	S.E.	Wald	df	Sig.	Exp (B)
Threats/severity to security issues	5.388	3.023	3.177	1	0.075	218.759
Security awareness	1.253	1.321	0.899	1	0.343	3.501
Benefits derived from behavioural change	0.39	1.119	0.121	1	0.728	1.476
Ability to change behaviour	1.568	0.898	3.05	1	0.081	4.799
Constant	-35.576	17.383	4.188	1	0.041	0.000

The variables involved in the model are shown in table VIII. The highest odds ratio (Exp(B)) in the model i.e. 218.759 corresponds to threats/severity to security issues (the variable with highest magnitude in predicting the outcome. This suggests that customers are more likely to change behaviour as a result of knowing the threats and severity of security issues. The model estimates an unknown probability of good behaviour, p, for any given linear combination of the independent variables with probability of bad behaviour, q, is given by q=1-p.

Considering the probability of an event that depends on four (4) covariates or independent variables for modeling the likelihood of good behaviour, the Logit(p) is given by;

$$Logit\,(p) = \ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 \qquad (1)$$

Where;

β_0 = Constant of the model

β_1 = Coefficient of independent variable x_1 (Threats/severity to security issues)

β_2 = Coefficient of independent variable x_2 (Security Awareness)

β_3 = Coefficient of independent variable x_3 (Benefits derived from behavioural change)

β_4 = Coefficient of independent variable x_4 (Ability to change behaviour)

Therefore;

$$\frac{p}{1-p} = e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4} \qquad (2)$$

$$p = (1-p)e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4} \qquad (3)$$

$$p = e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4} - \left(e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4}\right)p \qquad (4)$$

$$p + \left(e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4}\right)p = e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4} \qquad (5)$$

$$p = \frac{e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4}}{1+e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4}} \qquad (6)$$

Thus, the estimated regression equation for 4 independent variables is given by;

$$p = \frac{e^{-35.58+5.39x_1+1.25x_2+0.39x_3+1.57x_4}}{1+e^{-35.58+5.39x_1+1.25x_2+0.39x_3+1.57x_4}} \qquad (7)$$

Equation (7) therefore predicts the probability of good behaviour, p, given any linear combination of the independent variables. As compared to the original overall predictive ability of 59.3 without any predictive variables, the model is able to correctly predict 85.2% of the actual outcomes, which is pretty good.

IX. CONCLUSIONS AND RECOMMENDATIONS

The primary purpose of this study was to explore customer behavioural issues that are likely to impact internet banking security. The research used Ghanaian internet banking users as survey targets. The findings, however, contribute to the literature on internet banking security from customers' behavioural perspective. The theoretical framework for this study was the Health Belief Model. The model employed various factors such as demographic variables, threats/severity to security issues, security awareness, benefits derived from behavioural change and the confidence/ability to change behaviour (self-efficacy) as important elements in predicting customers' behaviour towards internet banking.

The findings from the study reveal that the demographic factor, gender, does not have any relationship with internet banking security breaches. This is inconsistent with the findings from a similar, past study [24]. Significant to this study is the evidence that customer behaviour is directly related to internet banking security breaches. As a result, customers need to behave in ways to minimize internet banking security issues. This finding is consistent with [25], concluding that security breaches will certainly influence internet users' online behaviour in increasing protection of their privacy and minimizing their exposure to security threats (p.73). These results have some implications for the banking sector in Ghana. First, the findings from the study will help banks to develop appropriate strategies in managing the various risks as a result of customers' behaviour on internet banking platforms. Banks therefore need to send out regular security tips to their customers in a bid to limiting customers' internet banking security breaches, which could affect the reputation of the banks. These security tips could also be displayed as banners on the internet banking platforms. Secondly, it is worth noting that internet banking security breaches do not necessarily emanate from unsecured measures on the part of banks, but also, as a result of inappropriate behaviour of customers on internet banking platforms. This is supported by [26], stating that security breaches are not only because of banks' faults and inadequate polices but customers are equally responsible for it, because customers' awareness regarding security is equally important (p.1016). Therefore, in order to remain competitive in the market, banks need to organize formal security awareness programmes aimed at instilling good customer behaviour on internet banking platforms. This is so essential to minimize the occurrence of security breaches that are likely to drive customers away, though the breaches may be as a result of their own actions or inactions. To avert these customer attritions, banks first need to convey a secure and reliable image by incorporating security elements in online services and communicate them to customers in a bid to guaranteeing confidentiality [27]. This is supported by [28] indicating that, banks must ensure that consumers feel safe when using online banking features (p.12).

In an attempt to predict customers' behaviour on internet banking platforms, the study made use of relevant constructs of the underlying theoretical model. These include threats/severity to security issues, security awareness, benefits derived from behavioural change and the confidence/ability to change behaviour (self-efficacy). According to the results of the regression analysis, threats/severity to security issues is the most significant predictor of customer behaviour on internet banking platforms. This suggests that customers are mainly concerned with internet banking security issues if they are well informed of the severity the threats pose to them. Banks therefore need to ensure that customers are well educated on the severity of the security threats they are exposed to, should they fail to behave appropriately on internet banking platforms.

The findings and their implications were obtained from a single study that examined internet banking behaviour of customers from a specific commercial bank in Ghana. The study also examined responses from a small sample size. It is therefore essential to exercise caution when generalising the findings of this study. These limitations pave the way for future research. First, future research should seek a larger sample size for more credible results. Secondly, it will be useful to conduct a complementary study to reveal other factors that could be considered in predicting the behaviour of customers on internet banking platforms.

REFERENCES

[1] A. Jain and S. Kalyanam, "Using Insurance to Mitigate Cybercrime Risk: Challenges and recommendations for insurers." 2012.

[2] I. Ivan, C. Ciurea, M. Doinea, and A. Avramiea, "Collaborative Management of Risks and Complexity in Banking Systems," *Inform. Econ.*, vol. 16, no. 2, pp. 128–141, 2012.

[3] United Nations Office on Drugs and Crime, *The globalization of crime [electronic resource] a transnational organized crime threat assessment*. Vienna: United Nations Office on Drugs and Crime, 2010.

[4] The National White Collar Crime Center, *Internet Crime Report*. United States of America: Internet Crime Complaint Centre, 2010.

[5] Bank of Ghana, "Licensed Banks, Representative Offices & their Registered Offices in Ghana - December 2015." Bank of Ghana, 2015.

[6] PricewaterhouseCoopers, "2014 Ghana Banking Survey," 2014.

[7] M. Mukhtar, "Perceptions of UK Based Customers toward Internet Banking in the United Kingdom," *J. Internet Bank. Commer.*, vol. 20, no. 1, 2015.

[8] P. Malhotra and B. Singh, "An analysis of Internet banking offerings and its determinants in India," *Internet Res.*, vol. 20, no. 1, pp. 87–106, Feb. 2010.

[9] T. Pikkarainen, K. Pikkarainen, H. Karjaluoto, and S. Pahnila, "Consumer acceptance of online banking:An extension of the technology acceptance model," *Internet Res.*, vol. 14, pp. 224–235, 2004.

[10] W. Nasri, "Factors Influencing the Adoption of Internet Banking in Tunisia," *Int. J. Bus. Manag.*, vol. 6, no. 8, Aug. 2011.

[11] A. K. Kazi and M. A. Mannan, "An empirical study of factors influencing adoption of Internet banking among students of higher education: Evidence from Pakistan," *Int. J. Finance Bank. Stud. ISSN 2147-4486*, vol. 2, no. 2, pp. 87–99, 2013.

[12] S. Mansumitrchai and C. Chiu, "Adoptation Of Internet Banking In Uae: Factors Underlying Adoption Characteristics," *Int. J. Manag. Mark. Res.*, vol. 5, no. 1, pp. 103–115, 2012.

[13] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, 2009.

[14] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[15] M. Chan, I. Woon, and A. Kankanhalli, "Perceptions of information security in the workplace: linking information security climate to compliant behavior," *J. Inf. Priv. Secur.*, vol. 1, no. 3, pp. 18–41, 2005.

[16] Y. Li and M. T. Siponen, "A Call For Research On Home Users' Information Security Behaviour.," in *PACIS*, 2011, p. 112.

[17] I. M. Rosenstock, V. J. Strecher, and M. H. Becker, "Social learning theory and the health belief model," *Health Educ. Behav.*, vol. 15, no. 2, pp. 175–183, 1988.

[18] Strecher, J. Victor, and I. M. Rosenstock, "The health belief model," *Camb. Handb. Psychol. Med.*, pp. 113–117, 1997.

[19] Comptroller of the Currency Administrator of National Banks, *Internet Banking Comptroller's Handbook*. 1999.

[20] S. Malempati and S. Mogalla, "User Authentication using Native Language Passwords," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 6, pp. 149–160, Nov. 2011.

[21] E. Grau, "Using factor analysis and Cronbach'salpha to ascertai n relationships between questions of a dietary behavior questionnaire," in *Proceedings of the Survey Research Methods Section, ASA*, 2007.

[22] J. A. Gliem and R. R. Gliem, "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales," 2003.

[23] S. Eurobarometer, "Cyber Security," *Belg. TNS Opin. Soc.*, 2015.

[24] D. K. Maduku, "Predicting retail banking customers' attitude towards Internet banking services in South Africa," *South. Afr. Bus. Rev.*, vol. 17, no. 3, pp. 76–100, 2014.

[25] A. J. Chin, S. A. W. S. K. Wafa, and A.-Y. Ooi, "The effect of internet trust and social influence towards willingness to purchase online in Labuan, Malaysia," *Int. Bus. Res.*, vol. 2, no. 2, p. p72, 2009.

[26] R. K. Jassal and R. K. Sehgal, "Online Banking Security Flaws: A Study," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 8, pp. 1016–1021, 2013.

[27] C. B. Ho and W. Lin, "Measuring the service quality of internet banking: scale development and validation," *Eur. Bus. Rev.*, vol. 22, no. 1, pp. 5–24, Jan. 2010.

[28] G. D. Williamson and G. E. Money–America's, "Enhanced authentication in online banking," *J. Econ. Crime Manag.*, vol. 4, no. 2, pp. 1–42, 2006.

Bright Kwame Ameme, received B.Sc. (Hons.) (Computer Science) from Kwame Nkrumah University of Science and Technology, Kumasi, Ghana , MBA (Finance) from Central University College, Accra, Ghana and a Ph.D. Fellow at Ghana Technology University College, Ghana. He has over 13 years experience in ICT management in the banking industry. His current research interest is on Internet Banking and Information Security.

Dr. Ezer Osei Yeboah-Boateng, FHEA, is a senior lecturer and the Head (Acting Dean), Faculty of Informatics, at the Ghana Technology University College (GTUC), in Accra. Ezer is a Telecoms Engineer and an ICT Specialist; an executive with over 25 years of corporate experience and about 8 years in academia. He has over 10 peer-reviewed international journal papers to his credit. His research focuses on cyber-security vulnerabilities, digital forensics, cyber-crime, cloud computing and fuzzy systems.