LEARNING THE LESSONS FROM THE DEVELOPED WORLD: E-BANKING SECURITY IN NIGERIA

Mumin Abubakre

Doctoral Researcher, Business School, Loughborough University, UK

Email: M.A.Abubakre@lboro.ac.uk

Crispin Coombs

Lecturer in Information Systems, Business School, Loughborough University, UK

Email: c.r.coombs@lboro.ac.uk

Chanaka Jayawardhena,

Senior Lecturer in Marketing, Business School, Loughborough University, UK

Email: C.Jayawardhena@lboro.ac.uk

Alan Hunt

Lecturer in Information Management, Aberdeen Business School, Robert Gordon University, UK

Email: a.hunt@rgu.ac.uk

Abstract

In the past decade banks invested heavily in internet technology so as to engage in e-business and e-commerce activities. However, this development exposed banks to threats, such as online fraud. Consequently, there was a need to adopt security measures and controls to mitigate such threats. Banks in developed countries have developed a level of 'best practice' to reduce such online threats. The objective of this study was to explore the extent to which banks in the developing world were benefitting from the experiences of banks in the developed world in terms of how they address online security threats. Case studies of two Nigerian Banks were undertaken using interviews and short questionnaire. The findings show respondents perceived the level of threats to e-banking in Nigeria to be low. When adopting e-banking security controls, the case study banks placed more emphasis on the technical dimension than the human dimension. Senior management commitment is a significant barrier to adopting best practice, which is highlighted in limited financial resources being provided for new investment in training or customer education. The study concludes that senior managers need to change their perceptions and priorities towards IT security to reduce the vulnerability of their e-banking services.

Keywords: E-banking, Security, Nigeria, Case Study.

LEARNING THE LESSONS FROM THE DEVELOPED WORLD: E-BANKING SECURITY IN NIGERIA

Abstract

In the past decade banks invested heavily in internet technology so as to engage in e-business and e-commerce activities. However, this development exposed banks to threats, such as online fraud. Consequently, there was a need to adopt security measures and controls to mitigate such threats. Banks in developed countries have developed a level of 'best practice' to reduce such online threats. The objective of this study was to explore the extent to which banks in the developing world were benefitting from the experiences of banks in the developed world in terms of how they address online security threats. Case studies of two Nigerian Banks were undertaken using interviews and short questionnaire. The findings show respondents perceived the level of threats to e-banking in Nigeria to be low. When adopting e-banking security controls, the case study banks placed more emphasis on the technical dimension than the human dimension. Senior management commitment is a significant barrier to adopting best practice, which is highlighted in limited financial resources being provided for new investment in training or customer education. The study concludes that senior managers need to change their perceptions and priorities towards IT security to reduce the vulnerability of their e-banking services.

Keywords: E-banking, Security, Nigeria, Case Study.

1 Introduction

The worldwide banking industry has seen high levels of investment in the adoption and use of technology in the last decade (Zhu et al., 2004). This new technology has enabled banks to improve their existing processes in terms of efficiency and reliability while also opening up new opportunities such as e-business and e-commerce activities. Many banks are now conducting many of their traditional business activities via the internet. As a result, these banks are now more exposed to online security threats (Workman et al., 2008). Therefore, it is important that banks adopt adequate security measures and controls to mitigate such threats (Hawser, 2007).

The banking industry in developed economies such as USA, UK and Hong Kong have implemented IT security strategies to respond to the online threats that arose from introducing internet banking services (Yiu et al., 2007). These security strategies are important not only for their primary goal of defending the banks IT systems, but also in ensuring high levels of customer trust and confidence in the use of e-banking. Therefore, security control measures can have a positive impact on a banks value chain activities, such as coordination to improve customer relationships (Lederer et al., 2001) and operational efficiencies to improve staff productivity (Chircu and Kauffman, 2000). Consequently, the banking industry in developed economies has experience and some success in mitigating online security threats.

Since the 1990s, the commercial banking industry has continued to grow with increasing speed in the major developing countries. This rise largely reflected the dramatic fall in inflation and financial liberalization (Hanson, 2003). In Nigeria, the banking industry is seeing high levels of growth, with new regulatory controls introduced in 2004 making banks stronger and enabling them to establish partnership working with foreign banks to manage the country's foreign reserves. Since 2004, Nigerian banks have invested heavily in their technology infrastructures with a desire to establish e-banking to provide value-added products and services such as internet banking and deployment of ATMs (Chiemeke et al. 2006). There was also a market-pull for e-banking in Nigeria from consumers due to the increased popularity and use of the internet. Access to the internet in Nigeria has grown significantly from 200,000 users in 2000 to 11 million users in 2009; making it the country with the second largest online users in Africa (Internet World Stats, 2009). However, the global nature of online security threats mean that banks that are relatively inexperienced in e-banking, such as those operating in developing economies, present new and possibly easier targets for online criminals, as banks operating in developed economies become more secure. Indeed, there are already examples of online fraud in Nigeria, with First Atlantic Bank Limited reporting a loss of five million naira (equivalent £20,000) from a single case (Chiemeke et al. 2006). Consequently, the overall aim of this research was to explore the extent to which banks in the developing world were benefitting from the experiences of banks in the developed world in terms of how they address online security threats.

The structure and layout of this paper is: firstly, a brief review of relevant information system literature and a statement of the research questions for the project; secondly, a discussion of the research methods adopted; thirdly, the research findings are presented; fourthly, the results are discussed; and finally, their importance is assessed in the concluding section.

2 Contextual Background and Research Objectives

There has been considerable research undertaken concerning the security of IT systems for organisations in general. This research stream has identified a range of threats including natural disasters, theft of hardware/software, unauthorised access and human error (Loch et al., 1992). More recent threats identified include viruses, trojans, spyware, phishing, “cookie monster” and “man-in-the middle attacks” (Post and Kagan, 2000, Bose and Leung 2008, Goodin 2008) as well as hacking, identity theft, and cyber terrorism (Furnell and Warren, 1999). Other studies have tended to concentrate on the effectiveness of the methods used to secure information systems. The strategies advocated by these studies to mitigate online threats have tended to focus on the technical aspects of information system security. However, it is becoming apparent that an increasing number of studies are giving greater attention to the human dimensions of information systems security as well as considering technical dimensions.

In terms of the technical perspective, IT security methods have tended to involve the deployment of hardware, software, network infrastructures and biometric authentication systems. For example, banks in developed economies have increased their online security by deploying two-factor authentication in the form of hardware security tokens, one time password and digital certificates, and zero knowledge proof to prevent identity thefts (Bose and Leung 2008). Other methods include firewall technologies, virus protection, 2 way factor authentication process for customers, and on screen and mouse operated keypads to secure information by preventing malicious programs that log user keystrokes (Hutchinson and Warren 2003). More recently, banks in the UK including Lloyds TSB, Barclays and Royal Bank of Scotland have come up with innovative ways to increase the security of their online banking service by providing card readers to their customers for conducting internet banking (BBC 2008).

From the human perspective, Ward and Smith (2002) suggest that IS users are an important resource in dealing with information security and the success of combating online threats depends on the level of commitment from the users. Similarly, Diniz et al. (2005) describe employees as the weakest link in the security chain, and mainly responsible for most security system failures. Hagen et al., (2008) argue that greater attention needs to be given to awareness activities, developing a security culture, and the provision of education and training as well as more common activities such as deploying security policies, procedures and controls, if organisations are to have secure information systems. However, addressing the human dimension through methods such as ongoing awareness training, as well as introducing technical controls, can be a resource intensive exercise which may be one reason that some organisations are choosing to concentrate on technical security methods (Thomson and Von Solms, 2006). This may well be even more pronounced for organisations working in developing world economies where resource constraints are likely to be acute. For example, Abu-Musa (2004), found in his survey of IT security controls in Egyptian banks that IT Directors focused more on the technical aspects of IT security than on the behavioural and organisational aspects. Similarly, a survey by Hood and Yang (1998) on 14 banks in Shezen, China, engaging in online banking transactions, suggests that management were aware of security threats but did not take necessary actions to mitigate or reduce the risks. This lack of action was explained as being due to a lack of financial resources and skilled IT personnel.

Therefore, it can be argued that in terms of the research on IT security, there is an emerging form of 'best practice' that is being advocated by the literature. In addition, in the developed world economies, many banks have gained significant experience in mitigating e-banking threats. Consequently, banks operating in developing world economies may be well placed to adopt the latest versions and techniques regarding IT security controls, without having to undertake the same learning and development path that the early adopters in the developed world had to take - a term referred as "leapfrogging" (Davison et al, 2000). However, to date the adoption of IT security controls and procedures by banks in the developing world has been under researched.

Although banking operations started in Nigeria in 1892 with the African Banking Corporation (now called First Bank of Nigeria), conventional banking commenced in 1952 (Chiemeke et al 2006). In 2004 the banking industry experienced further regulatory change from the Central Bank of Nigeria (CBN) when it announced banks had to increase their capital base from 2 billion Naira (£8 million) to 25 billion Naira

(£100 million). This change resulted in the number banks falling from 81 to 24. The re-capitalisation exercise has made Nigerian banks stronger, and enabled 14 Nigerian banks to partner foreign banks in managing the country's foreign reserves (My Africa 2006). Examples, of these partnerships include, Access Bank and Commerzbank of Germany, First Bank of Nigeria and H.S.B.C (UK); IBTC Chartered Bank and Credit Suisse (Switzerland); and Zenith Bank and J.P. Morgan (USA). Indeed, some Nigerian banks like Zenith, GT, Stanbic IBTC and Access now have commercial offices in the UK, while United Bank Africa has an office in the USA, and illustrates the recent boom of the Nigerian banking industry.

After the banking reforms in 2004, Nigerian banks began to invest heavily in improving their information technology infrastructure with the intention of providing a wide range of value-added products and services such as ATMs and e-banking. It appears that Nigerian banks are keen to try to catch up with global developments in banking and in so doing, improve the quality of services for their customers by changing from manual to automated business systems (Chiemeke et al. 2006). Ayo and Babajide (2006) in their survey on Nigerian banks report that all twenty four Nigerian banks are now engaged in e-banking. However, it appears that the Nigerian banks are also encountering increasing levels of cybercrime. Olugbile (2008), reports that banks in Nigeria have lost over N1 billion (about £4,000,000) to online financial fraud, identity theft, system penetration by outsiders, data and network sabotage and denial of service attacks. Therefore, the Nigerian banking sector provides an ideal context in which to investigate e-banking security in the developing world. The objective of this research is to investigate the level of adoption of IT security controls for e-banking in Nigeria. Specifically, this research examines three interrelated research questions:

1. To what extent are Nigerian banks following best practice in terms of IT banking security?
2. To what extent are Nigerian banks addressing the technical and human aspects of IT security?
3. What are the barriers and facilitators to Nigerian banks adopting the best practice approaches to IT security?

It was envisaged that by exploring these issues it would be possible to provide valuable insights into the applicability of best practice techniques in IT security for the banking industry in Nigeria, and for banks operating in the developing world in general.

3 Research Method

A case study approach has been identified as being helpful in developing and refining generalisable concepts and frames of reference (Lawler et al., 1985). Similarly, Yin (1994) argues that a case study approach is appropriate for exploratory research and suggests that it can act as a useful prelude to further research. Therefore, a case study approach was chosen for this study. Galliers (1992) notes that case studies are usually restricted to a single event or organisation and that it is difficult to collect similar data from a sufficient number of similar organisations making it difficult to generalise from case study research. To address this problem, within the constraints of access and limited resources, two case studies were selected for this study.

The case study banks were purposively chosen because they were major banks in Nigeria, and had several years of experience of implementing e-banking. Bank X has a branch network of 63 branches, annual total earnings and shareholders' value of over £110 million and £340 million respectively; while Bank Y has a branch network of 170 branches, with annual total earnings and shareholders' value amounting to excess of £250 million and £750 million respectively.

In order to study the phenomenon in depth, enabling a rich description and revealing its deep structure (Cavaye, 1996) a mixed method approach was adopted for data collection, comprising of semi-structured interviews and a survey. Data was collected between July 2008 and August 2008.

The semi-structured interviews were conducted first with four key stakeholders in each bank. The participants were selected on the basis of their prior experience and involvement with e-banking implementation at a senior level. The semi structured interview schedule (see Appendix 1) comprised 16 open questions and the questions were sent to participants a week before the interview to aid recall and make the interview process more productive. The interviews were conducted via telephone rather than face to face because of limited resources preventing travel to Nigeria. In the vast majority of cases, the initial telephone interview was complemented by a follow-up phone call that was used to clarify issues and attain supplementary information. All the phone interviews were tape recorded and later transcribed verbatim. Details of the range of informants interviewed at each bank is provided in Table 1 below.

Informant	Bank X	Bank Y
Head of Information Technology Department (ITD)	✓	✓
Head of IT Security Unit	✓	✓
Head of Learning and Development	✓	✓
IT Systems Auditor	✓	✓
Totals	4	4

Table 1: Range of Informants Interviewed at Each Bank

The qualitative data analysis followed the three concurrent activities identified by Miles & Huberman, (1994, p. 10) of data reduction, data display and conclusion drawing/verification. This approach is necessary to ensure that the researcher does not become overloaded from unreduced data transcripts and their information processing abilities impaired (Faust, 1982). Data reduction was conducted on each interview transcript using mainly 'in-vivo' codes, that is, codes derived from phrases used repeatedly by informants (Strauss & Corbin, 1990). In-vivo codes (as opposed to codes determined prior to the analysis) are appropriate when the research is essentially exploratory and are more useful in identifying new variables than adopting constrained literature-based codes (Diamantopoulos & Souchon, 1996). In addition, marginal remarks were used during the coding period to add clarity and meaning to the transcripts as well as having the ability to help revise and improve the coding structure (Chesler, 1987). From the codes it was possible to develop a series of within-case matrix displays for each bank which allowed the main themes that emerged from the interviews to be identified.

To supplement the qualitative data collected, a short questionnaire was administered via e-mail in order to develop a better understanding of the prevalence of the themes identified from the interviews. The questionnaire consisted of eight closed questions (see appendix 2) and used either a 5 item Likert scale ranging from very high to very low, or a simple dichotomous scale of 'yes' or 'no'. In addition, respondents were given the opportunity to answer 'don't know' rather than forcing a response or risking non-response to questions. The email questionnaire was initially sent to the Head of the IT Department within both banks who were asked to forward the email on to all middle and junior managers in their departments. This process helped in achieving a good response rate for the questionnaire as shown in Table 2.

	BANK X	**BANK Y**
Total Questionnaires Distributed	38	**36**
Return Completed	30	**22**
Non-Response	8	**14**
Response Rate (%)	**79**	**61**

Table 2: Questionnaire Response Rates at Each Bank

As has been noted earlier, the questionnaire data was intended to supplement the interview data and not to test hypotheses. Therefore, although the data were analysed using the SPSS package to generate frequency counts this analysis has been combined with the qualitative analysis in order to develop a richer understanding of the range experiences of e-banking security at each case study bank. The following section presents the key themes that were identified in the case study banks drawing on both the interview and questionnaire data as appropriate.

4 Findings

4.1 Perception of Online Security Threats

One of the first themes to emerge from the data analysis was that the majority of participants from both banks were aware of common online security threats and of the belief that online banking threats were relatively low. Two respondents being Head of IT Security from both banks gave their opinions on the perceived threats banks face while deploying e-banking services.

Head of IT Security of Bank X stated:
"…top on the list are attacks from hackers and also false identity whereby somebody can gain the identity or information about some other users and try to use it to authenticate and use their resources".

"……cases of ID theft, somebody will steal your login credentials and probably access your accounts. And probably some phishing too, though not common in this part of the world but Phishing is also likelihood" (Head of IT Security: Bank Y).

The perception of low online banking threats was shared between both senior IT managers and auditors and middle and junior managers that responded to the questionnaire. This perception seemed to be based on the view that there had been only a limited number of online attacks on banks in Nigeria to date. For example,

'I do not think we have really had major problems, I heard there was one attack on one bank which I would not want to mention their name other than that I do not think it is really prevalent in Nigeria….maybe because of exposure and all that but I do not think it is that serious in Nigeria. I think it is still very low' (Head of IT Security: Bank X).

It was suggested that this perceived low level of online criminal activity was due to '*the criminals [having still] to perfect their skills'* (IT Systems Auditor: Bank X) and that the level of use and awareness of the internet was still low in Nigeria, with the Head of IT in Bank Y stating,

'Well right now I will say it is still low because the awareness of internet use is not there…to an extent people are still sceptical to online banking as well [and] connectivity is still a challenge… people make use of [e-banking] more to check their balances just to know what they have in their account so as to make a decisions on either to withdraw or not.'

However, there was an acknowledgement among interviewees that the risk of online attack for the banks was growing. These threats were partly generated by a lack of awareness from bank customers about basic security measures as they perform common banking operations. The Head of IT of Bank X, when commenting on the how he would rate the future online security threats in Nigeria stated,

'I would say that on the scale of 1-5, I will say it is 4, because even if the bank does all that it needs to do people are not [sufficiently] knowledgeable to protect themselves well. They don't keep their PINS, they don't watch where they display/disclose their card details, things like that, so it's high'

The IT System Auditor in Bank Y agreed that the threats to online security were high and added that this was due to existing weaknesses in the IT security infrastructure and the limited skills of the IT staff developing the security controls. In some cases he believed '*the causes of threats are even more knowledgeable than the personnel providing the security*.'

It would appear that although some key staff are aware of the growing and current threats to e-banking at both case study banks, the majority of respondents still consider the likelihood of online fraud occurring to be low.

4.2 Physical and Electronic Security Controls

Both banks have deployed both physical and electronic security to mitigate threats to online banking services. These controls included firewalls, proxy servers and email content filtering machines and well as investing heavily in anti-virus/patch management to secure their network infrastructure. In addition, both banks had adopted biometric controls to manage physical access to key locations. For example, the Head of IT in Bank X commented:

'We have biometrics installed on physical locations of the entrance of ITD, Server farm and network communication rooms that keeps a log of movement of people in those locations. Also passwords of all network infrastructures are randomly changed and access only to staff of IT security unit'

When asked about the level of data encryption and authentication processes, both banks were gradually introducing these measures, but still had further work to undertake. In terms of data encryption, the Head of IT at Bank X stated:

'We have a policy in place which is called the information classification policy which grades all information that is used in the bank. This policy provides regular awareness to users on how to classify information to ensure that information is only available for use by an authorised person. Also we make sure access to data are protected with users credentials which is set to expire every 14 days .The eventual phase which we are looking at is encryption in which all the information that is on our users work station is encrypted so that in case of any loss or theft of such information cannot be accessed by any other person. That is presently going on in our group head office in Johannesburg. Implementation has already started from there and should get to Nigeria gradually. We are hoping to implement before the end of the year'

In terms of authentication for accessing online banking services the Head if IT for Bank X commented that they were only using *'One way [authentication] for now, just username and password'*. Similarly, in Bank Y the Head of IT commented that they were adopting *'Normal user name and password for now, but for transfer of funds between accounts the 2 way [authentication] comes in with the use of a secret code'*. It is interesting to note that by adopting only one way authentication for its online banking service, Bank X does not yet meet the standards set by developing world banks for authentication, which means it is susceptible to easy attacks by online criminals. Also, although Bank Y is adopting limited 2 way authentication the secret code provided by Bank Y is not dynamically assigned for each transaction, resulting in online transactions not being as secure as they could be.

In addition, both banks appeared to be taking steps to test the technical security controls they had implemented for their e-banking services. Bank X appeared to be more proactive in conducting these tests due to an affiliation with a foreign bank in South Africa. While there were still further developments to be implemented in terms of technical security controls, it appears that the majority of interviewees felt that the banks were adopting sufficient technical controls for e-banking services at the time of the research. This view was reinforced from the data that was collected from the questionnaire survey.

4.3 Policies and Strategies

Both banks had IT strategies in place although there were mixed views on how effective they were. For example, the IT System Auditor in Bank X commented that, *'I think the policies/strategies are okay as [they] address user access rights, privileges and controls'*. Whereas, the IT System Auditor in Bank Y had the view that *'The policies need some fine tuning. A more detailed risk analysis and risk profiling should be carried out. This would bring about better policies and strategies for ensuring secure online banking'*.

Despite the concerns held by the IT System Auditor in Bank Y, it would appear that Bank Y is developing more robust security strategies as they are actively communicating their formalised information security strategies to their customers. In addition, Bank Y is bringing in expertise from external consultants in order to develop and enhance their customers' online banking security. The Head of IT in Bank Y stated:

'...we actually contracted to Price Waterhouse Coopers to work on our policies and strategies. It is a document based on the strategic objectives of the bank for the next five years starting from 2007-2012. To prevent ID theft [we need] to educate our customers when using the internet platform. We also provide online key board instead of using the key stroke where customers just drop and select instead of you actually pressing your keyboard which can reduce the threat of passwords being stolen'

4.4 IT Staff Training and Customer Awareness Initiatives

It appears from the data gathered that both banks ensured that their IT staff were sent for regular training on security threats. The frequency of these training sessions varied from at least once a year to more frequent training sessions supplemented with seminars and conferences as appropriate. The type of training also varied depending on the job role. Overall, the management view was that the training had been sufficient to offset any online security risks as demonstrated by the banks not having encountered any significant attacks that had been successful. For example, the Head of Learning and Development in Bank X stated: *'So far we have not any had any major case … that has come out of security in our IT system so we believe that there is a pay off already…'*. Bank X may also be benefitting from sending their IT staff to training outside Nigeria, to more developed countries such as South Africa, where there is greater knowledge and experience regarding responding to e-banking security threats. The findings also indicate that Bank X benefits from learning IT knowledge from its group's head office in South Africa as highlighted by Head of Learning and Development commenting '*We also liaise with our head office in South Africa for them to also understand the group IT security models or framework so that we can implement locally in Nigeria.'*

Interestingly, while the banks appear to have adequate levels of training for their IT staff regarding current security threats, there were some concerns that this training may not be sufficient to protect against future threat levels. The IT System Auditor in Bank Y highlighted this concern commenting,

'The current skill level of the Bank's IT Security staff may be called to question when the environment becomes much more competitive than it is right now. Fortunately, we have not yet evolved into the era of blatant hacking attempts and more sophisticated fraud attempts. Therefore, it is imperative that the Bank takes into consideration future threats so as to adequately prepare the IT Security staff for the future. In other words, the right skills are just not there yet'

Responses to the questionnaires from both case study banks also suggested that the current IT staff skill levels and training were adequate but not high. There were also concerns that there were insufficient numbers of IT security staff employed and that this may limit the effectiveness of the banks IT security.

It is interesting to note that both banks had made limited attempts to educate their e-banking customers about major online threats. For example, Bank X simply added a notice to their website warning of potential threats. Bank Y was slightly more pro-active, by sending emails and SMS phone alerts on a regular basis when a known threat was present. Therefore, it would appear that improving the general awareness of their customers of online security issues was still an area that required further development. However, the findings from the questionnaire analysis suggest that many managers in both banks considered their banks attempts to educate customers were sufficient, which may explain why neither bank is making significant progress in this area.

4.5 Barriers to Adopting Best Practice

From the comments of interviewees in Bank Y, it appears that senior management commitment is a significant barrier to adopting best practice in terms of IT security controls. This lack of commitment was manifested through, limited financial resources being provided for new investment in training or technology. This is surprising as of the two banks, Bank Y would appear to have been the more successful and pro-active at addressing e-banking security threats. For example, the Head of IT Security in Bank Y commented, *'Security issues are not too common, so people tend to take those things for granted; it takes a lot of justification for you to get management buying into security deployment'*. The IT System Auditor in the same bank added, *'In most environments, senior management does not often see the need to spend so much money on IT infrastructure for which they cannot see the immediate returns or reasons for such huge expenditure'*.

As well as limiting the level of financial resources for IT security a related issue was the lack of a dedicated budget for IT security. In Bank X, funding for e-banking security had to be included in the general IT budget for the Bank. Not ring-fencing the IT security budget meant that it had to compete directly against other priorities, which may help to explain the lower level of adoption of best practice security practices at Bank X.

Responses to the questionnaire in both case study banks also suggested that the staffing levels within the IT department were considered inadequate by many junior and middle managers. Consequently, the banks were dependent on external specialists for some of their IT security which was both costly and limited the levels of IT security controls that could be deployed, due to the need for external expertise for implementation and maintenance.

Interviewees in Bank X identified a different barrier to effectively deploying IT security controls, the low levels of computer literacy of their e-banking customers. Consequently, there was a concern articulated in Bank X that there needed to be a sensible balance struck between online security controls and how onerous these controls made the online banking experience for customers. The Head of IT in Bank X commented,

'I think the major thing is customers' ease of use because we don't want to make things very hard. Most customers are not very computer literate. They just want to be able to check their accounts easily. So one of the things we try to do is not to make the process very tedious and very stressful for the customers. So we try, as much as possible, to make it friendly. We also try not to compromise security too much, [but] you have to strike a balance with the two'.

This low level of computer literacy among e-banking customers may also be further compounded by the low levels of awareness regarding online security. Consequently, many e-banking customers may well resist complicated security processes if they perceive them to be unnecessary.

5 Discussion

The findings have identified a number of interesting results. It would appear that the majority of participants in both banks perceive there to be a low threat level currently in the Nigerian online banking industry, although some respondents did acknowledge that their systems were vulnerable and that the level of threat was likely to increase in the future. This is despite existing evidence of internet related fraud already costing the Nigerian banking industry 4 million pounds Okemi (2008). This should be an area of concern as it suggests a level of complacency toward e-banking security among Nigerian banks as they continue to expand their interests to other countries in Africa and further afield. This expansion and growth will make these financial institutions more visible across the world and it is likely that it will only be a matter of time before these vulnerabilities are exploited by cyber-criminals.

The findings from participants indicates that they are following the technical dimension of best practice in e-banking security to some degree, by deploying technologies such as PIX firewalls, Proxy servers, Cisco gateways, and the installation of antivirus and patch management to secure their network infrastructure. These measures taken by Nigerian banks to secure their network infrastructure match those taken by their foreign counterparts in the UK and the US (Hutchison and Warren 2003). The 2 way authentication process has been partially adopted by Bank Y. Bank X has not yet adopting the two way authentication process but there is evidence of learning regarding the adoption of technical security controls from banks in more developed countries, such as South Africa, where the extra security is a concern for use and convenience (Weir et al., 2008). Consequently, the findings suggest that the Nigerian banks are benefitting from 'leapfrogging' in some areas of technical development. However, there is more work required by the Nigerian banks to improve their security features, such as encryption tools for preventing hacking of data, enhanced biometric applications like voice recognition, before they achieve the same level of technical security controls adopted by their foreign counterparts.

In terms of the human dimension of best practice, it would appear that the Nigerian banks have been less successful. While it appears that the banks' IT security staff are adequately prepared to combat the current level of e-banking threats there was a clear acknowledgement that they could easily be vulnerable to more sophisticated threats due to a lack of regular and updated training. Similarly, there was relatively little effort made by the banks to improve customer awareness of online security threats. This indicates that management may be placing more emphasis on investing in technology rather than on future staff training needs or educating their customers. It has been noted that poorly trained staff can be the weakest link in the security chain (Diniz et al., 2005). It has also been argued that organisations have to ensure they have specific roles for their IT security staff, such as Incidence Response Managers and IT Security Managers to manage and handle online security threats (Herrera 2006). This study's findings suggest that the two Nigerian banks investigated do have one of these roles (IT Security Manager) but that the other roles are have not been established. The lack of pre-emptive training for potential future online attacks may mean that the IT security staff in these banks may not even be able to recognise existing and potential threats.

The case study banks seemed to place more emphasis on the technical dimension of IT security by deploying necessary technologies to secure their online banking service, than on the human dimension of IT security. It is suggested that this difference in emphasis is largely due to technical security implementations incurring a one off cost compared to human issues that require continuous investment in the form of staff training and customers education. The example of Bank Y not sending regular SMS to its customers updating them on likely threats, illustrates the reactive nature of the strategies adopted. It is likely that the reactive approach by the banks is due to the perceived low level of online banking fraud within the Nigerian banking industry. Therefore it would appear that there has been less learning from the experiences of developed world banks, in terms of the human dimension of e-banking security despite links to foreign banks and consultants.

A range of barriers were identified by participants to the adoption of best practice in e-banking security. These barriers included a lack of senior management support, the high cost of deploying the required technologies, and balancing security with ease of use of systems by users and network infrastructure. These barriers are in line with studies conducted in other developing countries on the banking industry (Hood and Young, 1998). Other areas of concern included inadequate numbers of staff in the IT security unit and IT staff not having the skills to mitigate more sophisticated online threats when deploying online banking services. The majority of these barriers appear to relate more to the human dimension of e-banking security which again reinforces the view that the case study banks are more disposed to the technical aspects of IT security rather than the human aspects which neglects an important aspect of best practice in mitigating online threats adopted in the developed world.

6 Conclusions

This research has provided some important insights on the approach made by Nigerian banks in securing their e-banking services. Nigerian banks may not be fully adopting best practice by placing more emphasis on the technical dimension of e-banking security rather than having a balance between the technical and human aspects of e-banking security, as adopted by much of the developed world banking industry. However, the technical measures taken by the Nigerian banks does suggest that they are learning from their counterparts in developed countries, allowing them to move more quickly (leapfrogging) in their implementation of more complex IT security controls. However, the perception of low threat levels and crucially low levels of senior management commitment for more pro-active and pre-emptive security measures (such as greater training and customer education regarding new online threats), suggests that the Nigerian banking industry has further lessons to learn from the experiences of their developed world counterparts.

7 REFERENCES

Abu-Musa, A., (2004) Investigating the security controls of CAIS in an emerging economy- An empirical study on the Egyptian banking industry. *Managerial Auditing Journal*, Vol. 19 No.2 pp. 272-302.

Ayo, C. and Babajide, O. (2006). Designing a Reliable E-payment system: Nigeria a Case study. *Journal of Internet Banking and Commerce*. Vol.11 No. 2

BBC, (2008) A step up for online banking? [Online] Available from: http://news.bbc.co.uk/1/hi/programmes/working_lunch/7177502.stm [Accessed 04 September 2008]

Bose, I. and Leung, A., (2008). Assessing anti-phishing preparedness: A study of online banks in Hong Kong. *Decision Support Systems*.

Cavaye, A.L.M. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal*, 6, 227-242.

Chesler, M. (1987). Professionals' views of the "dangers" of self-help groups. *(CRSO Paper 345), Centre for Research on Social Organisation*. MI: Ann Arbor.

Chiemeke, S., Evwiekpaefe, A. and Chete, F. (2006). The Adoption of Internet Banking in Nigeria: An Empirical Investigation. *Journal of Internet Banking and Commerce*. Vol. 11 No.3

Chircu. A.M. and Kauffman. R.J. (2000). Limits to value in electronic commerce-related IT investments. *Journal of Management Information Systems,* Vol. 17. No. 2 pp.59-80.

Davison, R., Vogel, D., Harris, R. and Jones, N. (2000). Technology Leapfrogging in Developing Countries – An Inevitable Luxury? *The Electronic Journal on Information Systems in Developing Countries.* Vol. 1 No. 5. pp.1-10.

Diamantopoulos, A., & Souchon, A.L. (1996). Instrumental, conceptual and symbolic use of export information: An exploratory study of UK firms. *Advances in International Marketing, 8,* 117-144.

Diniz, E., Porto, M. and Adachi, T. (2005). Internet Banking in Brazil: Evaluation of Functionality, Reliability and Usability. *The Electronic Journal of Information Systems Evaluation*. Vol. 8 No. 1. pp. 41-50.

Faust, D. (1982). A needed component in prescriptions for science: Empirical knowledge of human cognitive limitations. *Knowledge: Creation, Diffusion, Utilisation, 3,* 555-570.

Furnell, S. M., and Warren, M. J. (1999), “Computer hacking and cyber terrorism: the real threats in the new millennium?” *Computer & Security,* Vol. 18 No. 1, pp 28-34

Galliers, R.D. (1992). Choosing information systems research approaches. In R.D. Galliers, (Ed.), *Information Systems Research*, London: Blackwell Scientific Publications, 144-162.

Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security.* Vol.16 No.4

Hanson, J.A. (2003) *Banking in Developing Countries in the 1990s*, World Bank Policy Research Working Paper 3168, available at: http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2004/03/30/000112742_20040330102739/Rendered/PDF/wps31680banking0in0developing0countries.pdf (accessed 22 December 2009).

Hawser, A., 2007. Banks on the spot over Internet Fraud. *Global Finance.*

Herrera, O., (2006). Personnel Profiles for Information Security Positions in Banks. *Bank Information Security.* [Online]. Available from: http://www.bankinfosecurity.com/articles.php?art_id=113&pg=1 [Accessed 28 June 2008]

Hood, K.L. and Yang, J-W. (1998). Impact of banking information systems security on banking in China: the case of large state-owned banks in Shenzhen economic special zone – an introduction. *Journal of Global Information Management*, Vol. 6 No.3, pp.5-15

Hutichson, D. and Warren, M., (2003) Security for Internet Banking: a framework. *Logistics Information Management*. Vol. 16 No. 1. pp. 64-73.

Internet World Stats. (2009). *Usage and Population Statistics*. [Online] Internet World Stats: Available from: http://www.internetworldstats.com/stats.htm [Accessed 16 November 2009]

Lawler, E. E., III, Mohrman, A. M., Jr., Mohrman, S. A., Ledford, G. E., Jr. and Thomas, G. Cummings and Associates (1985) *Doing Research That is Useful for Theory and Practice*, San Francisco, Ca.: Jossey-Bass.

Lederer. A, L., Mirchandani, D.A.; and Sims, K. (2001). The search for strategic advantage from the World Wide Web. *International Journal of Electronic Commerce.* Vol. *5.* No. 4 pp. 117-133

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding, *MIS Ouarterly.* Vol. 16 No 2, pp 173-86.

Miles, M.B., & Huberman, A.M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd Edn. London: Sage Publications.

My Africa, (2008). *Nigeria: Foreign Reserves - Gt Bank, 12 Others Get $7 Billion*. [Online]: Available from: http://myafrica.wordpress.com/2006/10/07/nigeria-foreign-reserves-gt-bank-12-others-get-7-billion/ [Accessed 08 September 2008]

Okemi, M., (2008) Nigerian banks lose N1 bn to cyber criminality – Expert. *Business Day Newspaper.* [Online]: Available from: http://www.businessdayonline.com/banking/15460.html [Accessed 01 September 2008]

Post, G., and Kagan, A. (2000), "Management trade-offs in anti-virus strategies", *Information & Management*, Vol. 37 No.1, pp.13-24

Strauss, A.L., & Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* Newbury Park, CA: Sage Publications.

Thomson, K-L. and Von Solms, R. (2006), "Towards an information security competence maturity model", *Computer Fraud & Security*, Vol. 2006 No.5, pp.11-15

Ward, P., and Smith, C.L. (2002), "The development of access control policies for information technology systems", *Computer & Security*, Vol. 21 No.4, pp.365-71.

Weir, C. S., Douglas, G., Carruthers, M. and Jack, M. (2008). User perceptions of security, convenience and usability for e-banking authentication tokens. *Computers & Security*. Vol. 28. No. 2009 pp. 47 – 62.

Workman, M, Bommer, W. H and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behaviour*. Vol. *24. No.* 6 pp. 2799- 2816

Yin, R.K. (1994). *Case Study Research: Design and Methods*. 2nd Edn, London: Sage Publications.

Yiu, C., Grant, K. and Edgar, D. (2007). Factors affecting the adoption of Internet Banking in Hong Kong—implications for the banking sector. *International Journal of Information Management*. Vol. 27. pp. 336-351.

Zhu, K. et al (2004). Information Technology Payoff in E-Business Environments: An International Perspective on Value Creation of E-Business in the Financial Services Industry. *Journal of Management information* system. 21(1) pp. 17-54.

APPENDIX 1: SEMI-STRUCTURED INTERVIEW SCHEDULE

1.0 Online Security Threats

1.1 How will you rate the security threats in online banking in Nigeria?

2.0 Awareness, Training and Education

2.1 Do IT staff undergo training on IT security?

2.2 How often do IT staff go on the training?

2.3 Does management feel the IT training on security is yielding the desired dividends?

2.4 Do you think IT security staff have the right skills to handle threats and breaches that arise from the bank deploying online banking?

2.5 Is the bank aware of phishing threats?

2.6 What is bank doing to educate customers on the threats of phishing?

3.0 Network Communication Infrastructure/Design

3.1 What kind of network infrastructure equipment is deployed to secure the network?

3.2 How does the bank physically secure the network?

3.3 Is the bank investing in anti-virus or patch management to secure the IT infrastructure?

3.4 What type of Authentication Process is deployed by the bank for its online banking customers?

3.5 Do you test the infrastructure deployed to secure your online banking service?

4.0 Policies and Strategies

4.1 Does the ITD have an incident response plan? When it was last updated and how often is it updated?

4.2 Does your department have a formalised information and security strategy? If it has, what are the actions adopted to prevent identity theft and online fraud on the network infrastructure?

4.3 What do you think of the policies and strategies that ITD has adopted to secure online banking?

4.4 How is IT security funded?

APPENDIX 2: SAMPLE OF ONLINE QUESTIONNAIRE

IT SECURITY IN NIGERIA'S ONLINE BANKING INDUSTRY: A CASE STUDY OF TWO BANKS

Please kindly letter bold your options in response to questions below.

KEY

VH – VERY HIGH
H - HIGH
M – MEDIUM
VL- VERY LOW
L - LOW

Y - YES
N – No
DK – Don't Know

1. Management Position
Middle Junior

2. How heavily is the online banking service used by its customers?
VH H M L VL DK

3. What do you feel is the extent of security threats and breaches to the online banking service?
VH H M L VL DK

4. Do you think the number of IT security staff are adequate enough to ensure the bank's online banking services are secured?
Y N DK

5. How well trained do you think the IT staff are to mitigate security threats and breaches when deploying online banking services?
VH H M L VL DK

6. Do you think IT security has deployed the right technology and processes to secure online banking services?
Y N DK

7. How effective are the bank's efforts at educating customers with regard to potential threats?
VH H M L VL DK

8. How significant a factor is security of the bank's network infrastructure with regard to it attaining market share?
VH H M L VL DK