Perceptions Towards On-line Banking Security: An Empirical Investigation of a Developing Country`s Banking Sector, how secure is On-line Banking

[1]Bongani Ngwenya [2]Khanyisa Malufu

[1]Dean, faculty of Business, Solusi University
Bulawayo, +263, Zimbabwe
/
[2]Department of Computers and Information Systems
Solusi University, Bulawayo, +263, Zimbabwe

Abstract

The increase in computer crime has led to scepticism about the move made by the banks to introduce on-line banking. Some view this as a noble move which has made the banking system more efficient, reliable and secure, while others view it as a risky and insecure way of banking. The aim of this study was to assess whether on-line banking in the developing countries is secure or not. The researcher chose a descriptive-quantitative research design. Data was collected using a self constructed questionnaire. Convenience sampling and stratified random sampling techniques were used to select the main subjects of the study. Generally on average there was no significant difference between the perceptions of management bank personnel and non-management bank personnel on the security of on-line banking. The study recommends further future studies on the security of on-line banking in developing countries based on the perceptions of the customers themselves, who are using on-line banking services, the Common Criteria for Information Technology Security and also a study of the latent dimensions of on-line banking security as extracted by factor analysis, how they differ from elements of information security as derived from the theoretical framework and literature.

Keywords: *on-line banking; on-line banking security; information security; network services; banking system*

1. Introduction

Information systems concentrate data in computer files that have the potential to be accessed by large numbers of people in and outside of organisations. While security breaches and damages of information systems still come from organisational insiders, security breaches are increasing, especially in developing countries because organisations are now open to outsiders through the internet. As a result, automated data are more susceptible to error, destruction, fraud and misuse.

The banking sector in Zimbabwe has introduced, of late, on-line banking facilities and these are heavily dependent on the use of internet. According to Laudon and Laudon [1] on-line banking, one of the systems involved in the movement of funds remains a subject to attack by natural and human threats. E-mail threats such as spam are well known, but there is another major entry point into a network, that is, the Web. As companies have become more adept at stopping e-mail threats, cyber-criminals have discovered new ways to infiltrate corporate networks through the internet. Research and Markets.Com (August 2004)[2] predicted that on-line banking will overtake traditional banking channels and become the single most important consumer banking channel. In internet banking system, the bank has a centralised database that is web enabled. Any organisation in e-business must consistently deliver great performance that matters to customers, raise customers` expectations and force all competitors to respond and generate rapid growth [3]. Furthermore, security and reliability are absolutely critical in systems for banking and financial services because errors, fraud, and disruption of service can lead to large monetary losses and the erosion of customer confidence in those companies and even the entire financial industry [1].

An introduction of on-line banking services in order to improve the efficiency in service delivery in the banking sector is to be welcome as a noble idea in Zimbabwe and the developing world in general, and a great step towards improving the performance of the banking sector in line with advancements in technology. Organisations that seek to make a difference should harness the latest technologies and stay abreast with the industry`s competition if they are to remain profitable with an edge or competitive advantage over their rivals.

In the order of consideration, the author first examines some insights from the literature and conceptual framework. Following the examination of the literature and the discussion of the conceptual framework, the researcher proposes research questions and related hypotheses that are tested using the Statistical Package of Social Sciences (SPSS).The research methodology is outlined, followed by the analysis of the data, and discussion. Finally, the conclusions are drawn and recommendations for further future research are made.

2. Literature review and theoretical framework

This section presents the theoretical framework, developed from literature upon which the concepts or themes of the study were based. The review of related literature cantered mainly on the risks associated with doing business on the internet. It also makes an examination and review of information pertaining computer security, computer crime, and the structure of information systems.

2.1 Information Security

Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. Furthermore, attacks come in various forms which may include loss of equipment due to theft or physical destruction, hacking, industrial espionage, or any other form [4]. According to Microsoft Corporation [5] common types of security vulnerability include using weak passwords, misconfigured software, social engineering, and unencrypted data transfer. On-line banking, like e-business or e-commerce requires flexible designs of the systems. Thus, the system has to be easily upgradeable, maintainable, and yet tightly secure.

O`Brien [6] states that the number one problem is security, and part of the problem is that the internet was developed for interoperability, not for impermeability. It is therefore very difficult to get maximum security as would be desired on the internet. As explained by Stamp [7], information hiding techniques such as steganography “hidden writing” and digital watermarking are another form of protecting information. Warwick [8] states that, traditionally information security has been considered to have three fundamental objectives:

- **Confidentiality** – ensuring that information is not disclosed or revealed to unauthorised persons.
- **Integrity** – ensuring consistency of data; in particular, preventing unauthorised creation, alteration or destruction of data.
- **Availability** – ensuring that legitimate users are not unduly denied access to information and resources.

2.1.1 Physical security

According to Peltier [9] physical security refers to securing the computer facility, its equipment, and software through physical means. These can include controlling access to the computer room by means of machine readable badges or a human sign-in\sign-out system; using closed-circuit television cameras to monitor computer areas; and backing up data frequently and storing backup in a fireproof, waterproof area.

2.1.2 Capital investment

Often the more secure or complex the solution, the more costly it is, and the more dependent on the third party that we have called to our aid [10]. Due to risks and threats that may lead to data loss or alteration, there is need to for serious backup so as to be protected from both physical and non physical destruction of data and the information system. Hence huge sums of capital investment are justified.

2.1.3 Access control

Forristal [11] suggests that access control basically deals with authentication and authorisation. However the problem with access control is that it cannot control how a resource may or may not be used after obtaining the access. For example, access control cannot specify that a given resource must be released after 15 minutes of possession. It is divided into two that is, the physical access control and the logic access control. Physical access control deals with the physical protection of buildings where the security guard is put in place to man the premises, closed circuit Televisions (TVs) are put in place to monitor and record the actions of anyone who enters the premises or restricted area, there is a logging system through use of passwords so that anyone who enters the server room is recorded or even through the use of access tags or security badges to gain access to some restricted areas.

2.1.4 Logical security

Logical security consists of software safeguards for an organisation`s systems, including user ID and password access, authentication, access rights and authority levels. These measures are to that only authorised users are able to perform actions or access information in a network or a workstation. According to Hurley [12] the unending string of data breaches and laptop thefts in recent months has shown, today`s threat landscape comprises far more than Distributed Denial of Service (DDoS) attacks, viruses and worms.

2.1.5 Security of network services

Although network has made the explosive growth of computer applications possible, the security liabilities it introduces are extremely problematic. In fact, a system`s network connection is the primary target of most modern security attacks. The hacker threat is a concern in all networks which have public network access or which use public network facilities [8].

2.1.6 Behavioural security

As stated by Laudon and Laudon [1] logical and physical controls are important but clearly not enough to provide adequate security. Behavioural changes are also necessary. The behavioural expectations of an organisation are encoded in its policy manuals and even on signs posted on bulletin boards. However the behaviour that organisation members internalise is also critical to the success of security efforts. Furthermore, employees should clearly understand what is expected of them, what is prohibited, and the extent of their rights and responsibilities [1].

2.1.7 Security policies

According to Layton [13] a security policy is a set of rules to apply to all security relevant activities in a security domain. He continues to suggest that if it important to be secure, then it is important to be sure all of the security policy is enforced by mechanisms that are strong enough. The security policy basically has one main objective and two controls. The control objective extends the scope to include relevant legal and regulatory aspects of an organisation`s business model. In particular, the information security policy document is considered to be the focal point of the program and has a dramatic effect on the overall security posture of any organisation.

2.1.8 Human resources competence

Lomash and Mishra [14] reiterate that, today, due to competition it has become quite difficulty to retain trained employees. It is in the light of the above fact, that it is possible that banks also lose qualified, trained and experienced employees who understand about information security. This challenges the security as they may replace them with untrained ones who may compromise the security standards. Other human limitations increasing system vulnerability include complacency and carelessness, greed, and limited ability to understand complex systems.

2.1.9 Organisational structure of the information systems department

Laudon and Laudon [1] suggest that management is responsible for developing the control structure and quality standards for the organisation. Key management decisions include establishing standards for systems accuracy and reliability, determining an appropriate level of control for organisational functions and establishing a disaster recovery plan. Many organisations that have realised the importance of the information systems have the director responsible for the information systems department.

2.1.10 Compliance

According to Layton [13] people in the organisation need to be informed of the risks that are possible in the organisation and the control measures put in place and also what is expected of them so that they can do it. If the responsible people in the organisation are aware of the risks and the control measures that have been implemented within their environment, it is reasonable to assume that there will be an environment of heightened awareness with the promise of fewer information security incidents [10].

2.1.11 Risk management

The key to controlling transaction risk lies in adapting effective policies, procedures, and controls to meet the new risk exposures introduced by e-banking. E-banking has unique characteristics that may increase an institution`s overall risk profile and the level of risks associated with traditional financial services, particularly strategic, operational, legal, and reputation risks. Management and personnel should understand the level of risk that exists within their environment and operations [13].

2.1.12 Disaster recovery plan

According to Laudon and Laudon [1] disaster recovery plan is a plan of action to recover from occurrences that shut down or harm major information systems. Laudon and Laudon go on to infer that, clients of telecommunications providers with computers and switching centres in or nearby the World Trade Center (WTC) lost service and were stalled with busy signals for at least three days when the WTC and the Pentagon were destroyed on the morning of September 11, 2001. However, Merrill was able to resume its business later in the day. The firm did not suffer as much as others because it had redundant telecommunications capabilities and a rock-solid disaster recovery plan. Whether provided by the financial institutions or a third party, management should plan for recovery of critical e-banking technology and business functions and develop alternate operating processes for use during service disruptions [15].

2.1.13 Customer retention

Petterson [10] suggest that it would be a good thing if the service provider would care more about profit in the long term, making clients happy, for the only good client is a happy client. An institution`s decision to offer e-banking services, especially the more complex transactional services, significantly increases its level of reputation risk.

2.1.14 Tight security

Security refers to the policies, procedures, and technical measures used to prevent unauthorised access, alteration, theft, or physical damage to information systems. Security can be promoted with an array of techniques and tools to safeguard computer hardware, software, communications networks, and data [1].

2.1.15 Quality data

According to Laudon and Laudon [1] there is a need to jealously guard the data in the organisation`s systems and maintain high quality data as data that are inaccurate, untimely, or inconsistent with other sources of information can create serious operational and financial problems for businesses, poor data quality may stem from errors during data input or faulty information system database design.

2.1.16 High availability

High availability computing are tools and technologies, including the backup resources for enabling speedy systems recovery from a crash. To provide the services efficiently and effectively, information technology infrastructures must provide a continuous level of service availability across distributed computing platforms...computer failures, interruptions, and downtime can translate into disgruntled customers [1].

2.1.17 Fault tolerance

Fault-tolerance or graceful degradation is the property that enables a computer based system to continue operating properly in the event of the failure of some of its components. Recovery from errors in fault-tolerant systems can be characterised as either roll-forward or roll-back. When the system detects that it has made an error, roll-forward recovery takes the system state at that time and corrects it, to be able to move forward. Roll-back recovery reverts the system state back to some earlier, correct version, for example using check pointing, and moves forward from there [1].

2.1.18 Customer satisfaction

According to Lucier and Torsilieri [3] any organisation in e-business must consistently deliver great performance that matters to customers, raise customer`s expectations and force all competitors to respond and generate rapid growth. A good system saves time whilst empowering the users. However, it has to be noted that, computer failures, interruptions, and downtime can translate into disgruntled customers [1]. Only satisfied customers can be retained.

2.1.19 Computer crime

Laudon and Laudon [1] suggest that computer crime is the commission of illegal acts through the use of a computer or against computer systems. The systems programmers, operators and administrators can disable protective features, replace the supervisors or reveal protective measures and thus making the system vulnerable to attacks. The maintenance staff can disable hardware devices or use the stand alone utility programs to attack the system. Thus the system is not safe even from the same hands which seek to protect it.

The researcher derived the following research question from the above literature and theoretical framework for the purposes of this paper:

Research Question: Is there a difference between the perceptions of management and non management on the adherence to elements of information security in implementing e-banking in Zimbabwe, as developing country?

3. Research Methodology

Questionnaires were distributed to 25 managers and 93 non managers from 8 commercial banks that offer e-banking services in Zimbabwe. Zimbabwe has 11 commercial banks; three of which currently do not offer e-banking services. The research used a quantitative descriptive method to assess the security of e-banking in a developing country. The samples used for the questionnaires were picked and chosen according to their years of experience and qualification in order to guarantee that they had the necessary computer skills and knowledge of e-banking. Evaluation and scoring of responses on the questionnaires is as shown in Figure 1 below.

`Scale	Responses	Verbal interpretation	Mean Interval
0	Very Strongly Disagree	Not implemented at all (1 chance in 100)	0.00 – 0.50
1	Strongly Disagree	Hardly ever the practice (1 chance in 10)	0.50 – 1.50
2	Disagree	Rarely the practice (2 chances in 10)	1.51 – 2.50
3	Slightly Disagree	Infrequent practice (3 chances in 10)	2.51 – 3.50
4	Very Slightly Disagree	Seldom practice (4 chances in 10)	3.51 – 4.50
5	Undecided	Neutral (5 chances in 10)	4.51 – 5.50
6	Very Slightly Agree	Occasional practice (6 chances in 10)	5.51 – 6.50
7	Slightly Agree	Often practice (7 chances in 10)	6.51 – 7.50
8	Agree	Usual practice (8 chances in 10)	7.51 – 8.50
9	Strongly Agree	Regular practice (9 chances in 10)	8.51 – 9.50
10	Very Strongly Agree	Consistent Usual Practice (99 chances in 100)	9.51 – 10.00

Figure 1: Evaluation and scoring of the questionnaires

Any score in the range of 8 and above were accepted as representing the perceptions of the respondents on the banks adherence to elements of information security in implementing e-banking in Zimbabwe as the respondents expressed that they agreed, whilst scores in the range of 7 and below were taken to mean that the elements of information security were not adhered to. The test value of 8.0 was therefore used as it is the minimum of the acceptable range of 8 to 10. Any values deviating from the test value were checked if they were on the upper or lower end. The higher values were showing that respondents strongly or very strongly agreed that the elements of information security were adhered to.

4. Analysis of Data

The table 1, below shows the demographic characteristics of the respondents in terms of their work experience.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid 0-3 years 4–6 years 7–9 years 10–12 years 13 years or more Total	6 16 18 5 3 48	12.5 33.3 37.5 10.4 6.3 100.0	12.5 33.3 37.5 10.4 6.3 100.0	12.5 45.8 83.3 93.8 100.0

Table 1: Respondents` work experience

The majority of the employees were experienced as the results show that at least 87.5% of the respondents had worked for the banks at least 4 years and they therefore understood better how the bank operates. They had observed at least how work is carried out, knew the organisational culture and at least knew the areas that are given greater priority in their organisations. This means that their responses were more accurate and a true representation of what actually takes place in their organisations. The table 2, below shows the demographic characteristics of the respondents in terms of their qualifications in information technology related training.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid None Certificate level	12 19 11 6 48	25.0 39.6 22.9 12.5 100.0	25.0 39.6 22.9 12.5 100.0	25.0 64.6 87.5 100.0

Diploma level				
Degree level				
Total				

Table 2: Information Technology related training

According to the results from the table 2 above, at least 75% of the respondents had some qualification and training knowledge in information technology. However, only 12.5% had pursued it to degree level. Their expectations and their judgement when it comes to the security of information systems was therefore considered to be more reliable as they responded to things they at least have heard of or actually work with in their day to day activities.

The rating or level of adherence to information security elements when implanting e-banking in Zimbabwe.

As shown in the table 3 below, a t-test was performed using a test value of 8.0 at 5% level of significance. Any scores in the range of 8 and above were accepted as representing that the certain elements of information security were adhered to, whilst scores in the range of 7 and below were taken to mean that certain elements were not adhered to. The test value of 8.0 was therefore used as it is the minimum of the acceptable range of 8 to 10.

Table 3: e-banking security (One-Sample T-test)

N = 48 df = 47 Test Value = 8.0

	Mean	Std. Deviation	Std. Error Mean	Sig. (2-tailed)	Mean Difference
Physical access controls	8.5764	1.57363	.22713	.015	.5764
Capital investment	8.7639	.90169	.13015	.000	.7639
Logical access control	7.0060	.89673	.12943	.000	-.9940
Security of network services	7.8194	1.23763	.17864	.317	-.1806
Behavioural security	7.2917	1.81487	.26195	.010	-.7083
Security policy	8.3083	.64042	.09244	.002	.3083
Human resources competence	8.2396	1.42821	.20614	.251	.2396
Organisational structure of IS department	9.5521	.48641	.07021	.000	1.5521
Compliance	8.0298	.88258	.12739	.816	.0298
Risk management and disaster recovery plan	8.6458	1.00403	.14492	.000	.6458
Average security	8.0818	.62347	.08999	.368	.0818

Any values deviating from the test value were checked if they were on the upper or lower end. The higher values were showing that respondents strongly or very strongly agreed that those particular elements of information security were adhered to. From the 10 dimensions that were tested, the following results were obtained:

Physical access control has a high mean of 8.6 which meant that on average, the respondents strongly agreed that their banks have physical access controls put in place and the results show that the level of control is significantly higher than the minimum expected.

Capital investment has a high mean of 8.8 and a low standard deviation of 0.9, meaning the respondents strongly agreed and all spoke with one voice that commercial banks are investing on the security of e-banking in Zimbabwe. There are backup communication networks, power sources and backup systems to ensure constant availability of information systems.

Logical access controls were significantly lower than expected with a mean of 7.0 and a standard deviation of 0.9 thus; respondents slightly agreed that logical access controls are put in place. There is a need for further analysis to find out which areas contributed to the low scores.

Security of network services were not significantly different from, though lower than the mean, which meant that banks met the network security requirements as expected for e-banking services to be conducted. However, there is still a room for improvement as they stood at the mean of 7.8 with a standard deviation of 1.2 when the required mean was 8.0.

Behavioural security stood at the mean of 7.3 and a high standard deviation of 1.8, which means most of the times banks fail to meet the requirements although on average, the respondents say often times the behavioural expectations are met. On this regard further analysis would need to be done in future.

Security policy as revealed by statistics in the table 3 above, indicated that banks have security policies in place that are approved by management and are reviewed from time to time. This is supported by a mean of 8.3, which is significantly high and a very low standard deviation of 0.6, thus banks are generally meeting the expectations in that area.

Human resources competence with a mean of 8.2 is though not significantly different, but higher than the test value of 8.0. Therefore, it can be concluded that the information technology staff at the banks are competent.

Organisational structure of information systems department has a high mean score of 9.6 and a very low standard deviation of less than 0.5. The respondents all spoke with one voice to say that banks have directors responsible for information technology departments, and though working closely linked and working together, information technology department is clearly separated from information technology security department.

Compliance is a very important element of information security. It is one thing to set policies and to have them followed is another. Banks as indicated by the results are managing to ensure that all sections of the organisation comply with the set standards and policies as shown by the mean of 8.01, which is not significantly different from the test value of 8.0. Thus, the respondents agree that compliance is ensured by the banks to make their e-banking services implementable.

Risk management and disaster recovery plan scored a significantly high mean of 8.6 with a very low standard deviation of 0.6 which meant that the respondents strongly agreed that commercial banks have disaster recovery plans and risk mitigation measures put in place to ensure critical information and information systems are available even in case of a disaster.

Generally, the average security level that was computed yielded a high mean of 8.08 which is not significantly different from the desired test value of 8.0, and a low standard deviation of 0.62 which means that on average elements of information security are adhered to ensure that e-banking is implantable.

Research Question: Is there a difference between the perceptions of management and non management on the adherence to elements of information security in implementing e-banking in Zimbabwe, as developing country?

There are basically ten elements of information security that were measured to determine if the perceptions of management and non management differ with respect to elements of information security. Table 4, below shows the mean scores of management versus mean scores of non management for each element that was measured.

Table 4: Group statistics for perceptions

	Current Position	N	Mean	Std. Deviation	Std. Error Mean
Physical access controls	Non	30	8.2667	1.62452	.29660
	management	18	9.0926	1.37582	.32428
Capital investment	Management	30	8.5222	.93335	.17041
	Non	18	9.1667	.69780	.16447
Logical access control	management	30	6.7286	.84253	.15382
	Management	18	7.4683	.80635	.19006
Security of network services	Non	30	7.4889	1.28872	.23529
	management	18	8.3704	.94204	.22204
Behavioural security	Management	30	6.8444	1.86258	.34006
	Non	18	8.0370	1.49897	.35331
Security policy	management	30	8.4600	.54114	.09880
	Management	18	8.0556	.72536	.17097
Human resource competence	Non	30	7.9000	1.44079	.26305
	management	18	8.8056	1.24722	.29397
Organisational structure of IS department	Management	30	9.6833	.40436	.07383
	Non	18	9.3333	.54233	.12783
Compliance	management	30	8.1857	1.02478	.18710
	Management	18	7.7698	.49763	.11729
Risk management and disaster recovery plan	Non	30	8.8000	.92027	.16802
	management	18	8.3889	1.10926	.26146
Average security	Management	30	7.9770	.63089	.11518

	Non management Management Non management Management Non management Management Non management Management	18	8.2566	.58649	.13824

The table 4 above shows the average scores for all items computed and the values obtained. These were summarised in variable, average security. This average security was used to determine the overall responses of the respondents as to whether or not they perceived that the elements of information security are adhered to. According to the overall average score there is no significant difference between the perceptions of management and perceptions of non management.

5. Conclusion and Recommendations

This study concluded that to a greater extent, the elements of information security are adhered to when implementing e-banking in Zimbabwe, as a developing country. However there is still some room for improvement in some sections with respect to elements of information security. Banks in developing countries need to improve on logical access controls and behavioural security as they were significantly lower than expected of banks that offer e-banking services.

The study recommends further future studies to include or find out the perceptions of the customers themselves who use e-banking services and the use of the Common Criteria for Information Technology Security. The study also recommends a further future study of the latent dimensions of e-banking security as extracted by factor analysis, to measure how secure e-banking is in Zimbabwe with respect to those factors.

References

[1] K. C Laudon, and J. P Laudon, “Management Information Systems-Managing the digital firm”. 8th ed. India: Prentice Hall 2004.

[2] Research and markets.com, “The E-payments and E-banking Market Outlook”. Retrieved September 8, 2008, from Web site: http//www.researchandmarkets.com/the-epayments-and-ebanking-market-outlook.htm.

[3] C. E. Lucier, and J. D Torsilieri, “Analysing Requirements and Defining Microsoft.net Solution Architectures: E-Business Microsoft Corporation”, Microsoft Press 2002.

[4] K. E. Kendal, and J. E. Kendal, “Systems Analysis and Design”. 5th ed. India: Prentice Hall.2004.

[5] Microsoft Corporation, “Analysing Requirements and Defining Microsoft.net Solutions Architectures”, Microsoft Press 2005.

[6] J. A. O`Brien, “Introduction to Information Systems”. 12th ed. Irwin: McGraw-Hill 2005.

[7] M. Stamp, “Information Security: Principles and Practice”. USA: John Wiley &Sons Inc 2005.

[8] F. Warwick, “Computer Communications Security: Principles, Standard Protocols and Techniques. USA: Prentice Hall. 1994.

[9] T. R. Peltier, “Information Security Risk Analysis”. USA: Auerbach Publications 2001.

[10] S. Petterson, “Database and network”, An International Journal of Database and network practice, vol.38, 2008, pp.9-23.

[11] J. Forristal, “Physical and Logical Security”. Retrieved May 24, 2009, from Web site: http//www.networkcomputing.com/show Article.jhtml?Articled=194200006, 2006.

[12] B. Hurley, “Physical and Logical Security”. Retrieved May 21, 2009, from Web site: http//searchsecurity.techtarget.com/news/article/0,289142,sid14-gci1241956,00.html, 2007.

[13] T. P Layton, “Information Security: Design, Implementation, Measurement, and Compliance”. USA: Auerbach Publications 2006.

[14] S. Lomash, and P. A Mishra, "Business Policy and Strategic Management". New Delhi, India: Vikas Publishing House (Pvt) Ltd 2005.

[15] Federal Financial Institution Examination Council, "IT Handbook InfoBase Booklet: E-Banking". Retrieved May 18, 2009, from W eb site: http://www.ffiec.gov/ffiecinfobase/booklets/e-banking/e-banking-03a-exam-points.htm 2009.