International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

The Effect of Cyber-Crime Response Costs on the Development of Financial Products: A Case of NIC Bank of Kenya

Elizabeth Njoroge[1], Dr. Agnes Njeru[2]

Jomo Kenyatta University and Technology, P.O. Box 620000-00200, Nairobi, Kenya

Abstract: ***Given the fact that the cost of doing business under the new ever changing information communication and technology platform, the question of this this research was whether these costs are deterring banks from operating in this new risky environments and platforms or to what extent are these affecting the rate at which banks are developing new ideas and products that are transacted on an online platform. The research proposal adopted one independent variable to help estimate these effect which includedResponse costs, and the rate of development and growth of financial products as the dependent variable. The study used a questionnaire where it was administered to establish the effect of these factor. The respondents/ population of this research proposal was 957 bank employees, inclusive of 167 support staff, at NIC bank of Kenya. The study used a case study of the NIC bank of Kenya through purposive. A sample of 10% out of the bank employees minus the support staff gave a sample size of 80 respondents. The interview guides was to be self-managed to allow for convenience and reliability of the data. A pilot study was done on the area of study in order to measure the validity and reliability of the data collection instrument. The study adopted a descriptive research design where SPSS was used to model the relationship between the various selected variables and test there explanatory power. After the analysis the data was presented through the use of various presentation tools such as graphs pie charts and tables.***

Keywords: Response cost, financial products, Kenya Commercial Bank

1. Introduction

The term ICT according to Zuppo (2012) that is information and communication technology can be defined as a combination of communication applications and procedures and devices that include phones, computer and network hardware and software. Milis & Mercken (2002) Information and communication technologies have been implemented in various sectors in the economy such as the education sector, health care, financial sector to aid in service delivery. Information communication and technology has been customized over the years to fit in all sectors as it is needed based on the services that each sector provides.

According to Reynolds, Treharne &Trippo (2003) the rate at which human beings are transitioning from manual operations is now increasingly depending on digital communication and other innovations in the information and communication industry. In the financial sector ICT has been influential in enabling financial institutions in extending its services through financial inclusion of people unreachable by this services and also diversifying its services (Pilat, Lee & Van Ark,2003).According to Agboola (2007) In this day an era people can now access simple services such as cash deposit and withdrawal, payment of bills and payment of other daily services from their phones, computers and other electronic devices that are being developed on a daily basis. Agboola (2007) connectivity therefore has increased enabling people to access market information, and relevant services which is helping to make life easier for people.

Information communication and technology has proved to be a powerful tool in extending economic opportunities to all individuals, groups, businesses and institutions all over the world (Stiroh, 2002). According to Avgerou (2003) information communication technology has contributed to the concept of global economic shrinkage in terms of allowing connectivity for people form any point on the globe. According to statistics all new mobile owners and customers in the coming generations will be mostly from developing and third world states which is an indication that the ICT platform is enabling connectivity from those who are well developed to those who are developing. According to Agboola (2007) today businesses and financial institutions that invest heavily in information and technology have a competitive edge in terms of being more productive, growing faster, more investment opportunities and more profits.

Kshetri (2005) despite all the benefits accrued or linked to the extensive usage of information technologies, the increased dependency has also translated into a growing rate of criminal activities conducted via the same ICT platform. Bell (2002) the expansion of cyber functionalities has, however, also opened up new opportunities for people to carry out criminal activities online, and/or to use the Internet as a medium for their criminal objectives. The advantages of the Internet come with risks. Kshetri (2005) while organizations and individuals are exploiting its business benefits they may not realize that cyberspace confers the same benefits on those who wish to attack them.

Much has been done on how information and communication technologies or cyberspace is beneficial to all sectors of an economy, less has been done on the criminal activities that characterize this new revolution and it affects the activities of institutions today such as development of new financial products. Kshetri (2005) the understanding of cybercrime and its consequences, both economic and

social, is still limited. Cybercrime has been also increasing at the rate at which new technological innovations are being invented. Bell (2002) users of ICT technologies have been facing lots of criminal activities recently from cyberspace as a result of the risk that lie within the information communication sector. The cost of this criminal activity have now reached a significant point where a need to address them is long overdue. As cybercrime becomes more of an issue many organizations seek to protect themselves using courses to train employees in the very real risks of the online world. This paper seeks to address this costs and how they are affecting the performance of banks today and more specifically the development of new bank products.

2. Statement of the problem

Recent studies published on the evolution ICT present concerning scenarios, characterized by the constant growth of cyber-criminal activities. Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to combat them, illegal profits have reached amazing figures. The impact to society has become unsustainable, considering the global economic crisis.

The proliferation of, and rapid advances in, technology-based systems, especially those related to the internet, are leading to fundamental changes in how companies interact with customers Kaigen et al, (2015). Internet banking has become the self-service delivery channel that allows banks and various other businesses to provide information and offer services to their customers with more convenience via the web service technology. Kaigen et al, (2015) in addition to this, the challenging business processes in the financial services pressurized banks to introduce alternate business channels to attract customers and improve customer perception. Kaigen et al, (2015) cybercrimes against banks and other financial institutions probably cost many hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information probably costs developed economies billions of dollars. Kaigen et al, (2015)these losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage. Kaigen et al, (2015) these costs are now greatly affecting the bottom line or profits generated from innovative activities by banks today. The above mentioned studies by Kaigen et al, (2015) plus other studies by Jackson et al (2004), and Kshetri (2005) only describe the economic impact in general, none of this studies narrow down to what costs banks are incurring as a result of cybercrime and how it is affecting performance and innovation. Therefore the study intends to establish the types, impact and mitigations of cybercrime related costs in the development of financial products in Kenyan Banks.

The General objective of the study

The general objective of the study was to investigate the effect of response cost on the development of financial products; a case of NIC bank of Kenya.

The Specific objectives of the study

1) To find out the effect of compensation payments on the development and growth of financial products by NIC bank in Kenya.
2) To evaluate the consequence of regulatory fines on the development and growth of financial productsby NIC bank in Kenya.
3) To establish the impact of legal costs on the development and growth of financial productsby NIC bank in Kenya.

3. Theoretical Review

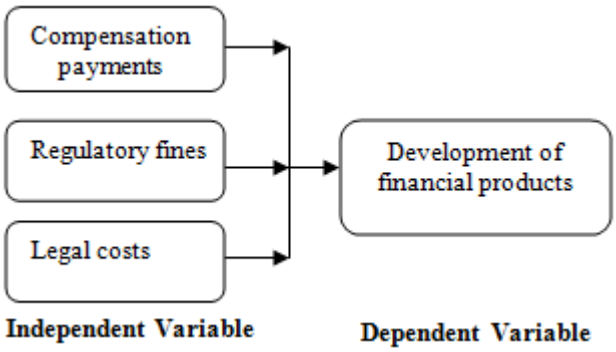
Space Transition Theory

This theory was developed by Jaishankar in 2007 and published in his book on Crimes of the Internet (Jaishankar 2007). There has been inadequate theoretical explanations as to why there is a rampant increase in cyber related crimes. This theory of space transition theory tries to give an explanation for the phenomena of cybercrimes. This theory states that people who usually feel there criminal nature is repressed by the physical space have a tendency to engage in crime in cyber space which otherwise they would not commit in a physical setting due to their status and role. This nature of crime is associated with characteristics such as identity flexibility, dissociative obscurity which make it easy for people to commit offenses. The emergence of and advancements in the field of information and communication technologies has created a range of new criminal activities within the economic and social space. All these activities have had a great impact on how financial institutions and more specifically banks are performing. As this theory states people involved in cyber related offenses are not hardcore but rather the white collar community who are within a closed community such as a bank. Detection becomes hard and the costs increase gradually at to a point where the impact on the intrusions bottom line is evident.

Therefore the postulations of this theory is that one of the factors contributing greatly to the increasing costs that banks are facing in relation to cyber space loopholes is the complex nature and characteristics and behavior of the offenders within the information and communication environment. The postulates of the theory are: Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape. Strangers are likely to unite together in cyberspace to commit crime in the physical space. Associates of physical space are likely to unite to commit crime in cyberspace. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes.

4. Conceptual Framework

The study adopted the following conceptual framework:



Source: Author 2017
Conceptual framework

Response cost

These takes into account direct losses to individuals and companies (including business continuity and disaster recovery response costs), and indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness. Consequential cost are those that have affected the banking institution directly (Anderson et al, 2013).

While companies fear reputation damage, there has been little work to quantify it. Companies suffer reduced valuation after public reporting of their being hacked, usually in the form of a drop in stock prices (Lewis & Baker, 2013). These losses can be significant—ranging from 1% to 5%—but appear not to be permanent. Stock prices usually recover by the next quarter. It would distort any calculation of loss to attempt to include these fluctuations in stock prices (Lewis & Baker, 2013).

However, it will be interesting to see if this changes as a result of new SEC regulations that require companies to report major hacking incidents, which may improve shareholder understanding about what hacks are commercially material (Lewis & Baker, 2013). Shareholders are unlikely to have good information about what was taken, let alone by whom and for whose benefit. Recovery of stock prices may not be so quick if investors decide that there has been significant damage to a company's intellectual property portfolio or if it sees a significant outflow of customers as a result (Anderson et al, 2013).

The most important area for loss is in the theft of intellectual property and business-confidential information economic espionage (Lewis & Baker, 2013). It is difficult, however, to precisely estimate the losses. This is in part because cyber spying is not a zero-sum game. Stolen information is not really gone. Spies can take a company's product plans, its research results, and its customer lists today, and the company will still have them tomorrow. The company may not even know that it no longer has control over that information (Lewis & Baker, 2013). There are many ways to determine the value of intellectual property. One is to estimate what it would fetch on the market if offered for sale or for licensing. Companies can value their intellectual property by determining the income streams it produces and is expected to produce in the future (Anderson et al, 2013).

Companies can also estimate what it would cost to replace intellectual property as a means of estimating its value, although a reliance on inputs for estimating value can be very misleading (Lewis & Baker, 2013). The actual value of intellectual property can be quite different from the research and development costs incurred in creating it (Lewis & Baker, 2013). If a company spends a billion dollars on a product that fails in the market, and a foreign power steals the plans, the loss is not a billion dollars but zero the invention's market value (Anderson et al, 2013).

Service disruptions, such as denial of service attacks, may have only a limited cost on a national economy (although they can be disruptive for the company that experiences them). If the website of an online retailer is taken offline, they will lose sales, but the actual economic effect may be much smaller (Lewis & Baker, 2013). Intellectual property (IP) losses are the most difficult to estimate for the cost of cybercrime, but it is also is the most important variable for determining loss. IP theft shifts trade balances and national employment. Countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs, and income from cybercrime (Lewis & Baker, 2013). The effect of cyber espionage on national security is significant, and the monetary value of the military technology taken does not reflect the full cost to victim countries (Anderson et al, 2013). Cybercrime damages innovation. One way to think about the cost from cybercrime is to ask how investors would act if returns on innovation doubled. Companies would invest more and the global rate of innovation would increase. By eroding the returns on intellectual property (IP), cybercrime invisibly creates a disincentive to innovation.
Stealing business confidential information—investment information, exploration data, and sensitive commercial negotiation data—can yield immediate gain (Lewis & Baker, 2013). The damage to individual companies runs into the millions of dollars. One UK Company told British officials that it incurred revenue losses of $1.3 billion through the loss of intellectual property loss and subsequently suffered a disadvantage in its commercial activities (Lewis & Baker, 2013). Hacking of central banks or finance ministries could provide valuable economic information on the direction of markets or interest rates (Anderson et al, 2013).

These costs include the relevant actions that a banking institution has to take to respond to the losses that may have been suffered by other parties such as customers as a result of an attack through the online platforms. These includes costs such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues (Anderson et al, 2013).

The cost of cleaning up after a cyber-attack may be relatively small. One survey by (Lewis & Baker, 2013) found an average of about $9 million for large companies to clean up after a successful breach. Many of those incidents were of the lost-laptop variety, and one might expect the

costs of curing actual cyber espionage intrusions to be much higher (Lewis & Baker, 2013). One area for further research is increased insurance costs, as companies seek to control liability for breaches of their networks (Anderson et al, 2013).

A calculation of the cost of malicious cyber activity would need to consider opportunity costs, forgone opportunities, or lost benefits that would otherwise have been obtainable for activities in cyberspace (Lewis & Baker, 2013). Additional spending on cyber security that would not be required in a more secure environment is one example of an opportunity cost. Other examples include lost sales or lower productivity, a decision to avoid the internet for some activities (Anderson et al, 2013).

A survey cited in the European Commission Cyber security Strategy Document found that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases and avoid revealing personal information because of security concerns (the greatest fear is over identity theft for purposes of financial fraud) (Lewis & Baker, 2013). A 2008 Study commissioned by the European Network and Information Security Agency (ENISA) found "growing public concerns about information security hinder the development of both markets and public services (Lewis & Baker, 2013)." A 2006 global survey taken by the International Telecommunication Union as part of its campaign to play a greater role in cyber security, based on 400 respondents, found that at that time, more than 40% of Internet users avoided some online transactions because of security concerns (Lewis & Baker, 2013). None of these figures are determinative, but they suggest that there could be forgone opportunities in the use of the internet for commercial purposes because of security concerns (Anderson et al, 2013).

Cleaning up cybercrime is expensive. The cost to individual companies of recovery from cyber fraud or data breaches is increasing. While criminals will not be able to monetize all the information they steal, the victim has to spend as if they could use all the stolen data (Lewis & Baker, 2013). The aggregate cost for recovery is greater than the gain to cybercriminals. One study of the cost of cybercrime for Italy found that while the actual losses were only $875 million, the recovery and opportunity costs reached $8.5 billion (Lewis & Baker, 2013). The bill for recovery costs is where the real damage to society begins, and the effect on a business can include damage to brand and other reputational losses and harm to customer relations and retention (Anderson et al, 2013).

Development of financial products

Technology has altered many aspects of financial transactions. In the area of lending, for instance, information on firms and individuals from a variety of centralized sources such as Dun and Bradstreet is now widely available. The increased availability of reliable timely information has allowed loan officers to cut down on their own monitoring. While, undoubtedly, some soft information that is hard to collect and communicate direct judgments of character, for example is no longer captured when the loan officer ceases to make regular visits to the firm, it may be more than compensated by the sheer volume and timeliness of hard information that is now available. Moreover, because it is hard information past credit record, accounting data, etc. the information can now be automatically processed, eliminating many tedious and costly transactions. Technology has therefore allowed more arm's length finance, and therefore expanded overall access to finance. Such methods undoubtedly increase the productivity of lending, reduce costs, and thus expand access and competition. Petersen and Rajan (2002) find that the distance between lenders and borrowers has increased over time in the United States, and the extent to which this phenomenon occurs in a region is explained by an increase in the bank loan to bank employee ratio in that region, a crude proxy for the increase in productivity as a result of automation.

Research Methodology

Descriptive research design was adopted in the study since it helps in achievement of measurable findings. Descriptive research involves gathering data that describe events and then organizes, tabulates, depicts, and describes the data collection (Kothari, 2004). The method was preferred because it allows for an in-depth study of the subject in a quantitative aspect of the overall research. Descriptive research design aims to gather data without any manipulation of the research context, focusing on individual subjects and going into depth and detail in describing them. In the study the variables included loan size, loan term as well as interest rate which were analyzed further by use of the named research design.

The study targeted the NIC bank of Kenya as its main case study. This was based on the purposive population selection technique since the study was more interested in extreme cases of bank fraud that provides the purest most clear-cut instance of the phenomena the researcher is interested in. NIC Bank had over 24 branches in Kenya. The respondents of this research proposal were employees in NIC bank in Kenya drawn from the 24 branches. Therefore, 80 participants were selected randomly from the employees to respond to the questionnaire.

The researcher employed the use of questionnaires in gathering firsthand information from the respondents which comprised of open ended questions to allow ease in data analysis, interpretation and tabulation of the questionnaires, and the closed ended questions which restricts respondents to yes and no answers. The instrument of research was then distributed prior to the actual research date in order to test the validity of the question and the availability of the respondents in a pilot study.

The completed questionnaires were edited for completeness and consistency. The data was then coded to enable the responses to be grouped into various categories. Data collected was purely quantitative and it was analyzed by descriptive analysis methods such as measure of central tendency e.g. mean, mode, median and measure of dispersion e.g. standard deviation, ration as well as percentages. The descriptive statistical tools assisted in describing the data and determining the extent to be used.

Data analysis also used SPSS to generate quantitative reports. The researcher then presented the analyzed data through tables, pie charts, and graphs.

5. Results and Discussions of the Findings

Organizational values

Table of Response cost to cyber-crime; (Compensation payments, regulatory fines, legal costs)

	N	Minimum	Maximum	Mean	Std. Deviation
Banks are required to compensate victims of identity theft whose information has been hacked; these increases the banks costs hence regulating the adoption rate of some of products, services and processes being innovated.	80	2	5	3.75	.703
There are numerous regulatory fines that are associated with lack of compliance to some of the standards issued by the banking oversight committee which affects the rate at which banks adopt innovated products, services and processes.	80	2	4	3.60	.739
Banks fear the costs that they may incur from legal suits directed towards them by affected parties of cyber-attacks, hence cautious on the adoption of new products and services.	80	2	5	3.65	.797
Legal forensic issues associated with cyber-criminal activities may lead to the closure of the entire business, therefore banks are cautious on what to adopt in terms of newly innovated banking products and services	80	2	5	3.55	.810
Legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services	80	2	5	3.60	.866

6. Summary of the Findings

According to study findings in Table 4.6, in average the respondents agreed that banks are required to compensate victims of identity theft whose information has been hacked; these increases the banks costs hence regulating the adoption rate of some of products, services and processes being innovated as shown by a mean of 3.75 and standard deviation of 0.703, in average the respondents agreed that there are numerous regulatory fines that are associated with lack of compliance to some of the standards issued by the banking oversight committee which affects the rate at which banks adopt innovated products, services and processes as shown by a mean of 3.60 and standard deviation of 0.739.

On average the respondents agreed that banks fear the costs that they may incur from legal suits directed towards them by affected parties of cyber-attacks, hence cautious on the adoption of new products and services as shown by a mean of 3.65 and standard deviation of 0.797, respondents agreed that legal forensic issues associated with cyber-criminal activities may lead to the closure of the entire business, therefore banks are cautious on what to adopt in terms of newly innovated banking products and services as shown by a mean of 3.55 and standard deviation of 0.810, further the respondents agreed that legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services as shown by a mean of 3.60 and standard deviation of 0.866. This findings indicated that banks fear the consequence of dealing with a cyber-attacks supported by (Anderson et al, 2013). This was an indication that issues such as recovery of stock prices may not be so quick if investors decide that there has been significant damage to a company's intellectual property portfolio. Despite this assertion and finding, Lewis and Baker (2013) were opposed to this findings claiming that the cost of cleaning up after a cyber-attack may be relatively small.

7. Conclusions

The study established Response rates costs was a significant predictor of Development of financial products as indicated by the p-value. The study showed that there was a high percentage chance of decrease in development of financial products as a result of increase in response costs. Banks consider a lot of factors when it comes to offering highly innovated services and products that customers need. These costs include the relevant actions that a banking institution has to take to respond to the losses that may have been suffered by other parties such as customers as a result of an attack through the online platforms. As observed by other researchers most of these costs includes costs such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues. The findings of these study, although were in contradiction with other studies who stated that the cost of cleaning up after a cyber-attack may be relatively small.

8. Recommendations

The study observed that the aftermath of a cyber-attack is characterized by a number of stake holders being affected not just the bank. The study recommends that banks should enter into agreements with other financial institutions that provide insurance cover to provide insulation over some of the costs that banks face in order to prevent reduction of operations hence resulting loss of revenue.

References

[1] Agboola, A. (2007). Information and communication technology (ICT) in banking operations in Nigeria–An evaluation of recent experiences. African Journal of Public Administration and Management, 18(1), 1-102.
[2] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M. & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information

security and privacy (pp. 265-300). Springer Berlin Heidelberg.
[3] Avgerou, C. (2003, May). The link between ICT and economic growth in the discourse of development. In Proceedings of the International Federation of Information Processing, IFIP (Vol. 9, pp. 373-386).
[4] Bell, R. E. (2002). The prosecution of computer crime. Journal of financial crime, 9(4), 308-325.
[5] Jaishankar, K. (2007). Establishing a theory of cybercrimes. International Journal of Cyber Criminology, 1(2), 7-9.
[6] Kaigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., & Siyanda, S. (2015). Kenya Cyber Security Report 2015. Serianu Limited.
[7] Kothari, C. (2004). Research Methodology, Methods and Techniques. New Delphi: International P Limited.
[8] Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541-562.
[9] Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. Center for Strategic and International Studies, Washington, DC, 103-117.
[10] Milis, K., &Mercken, R. (2002). Success factors regarding the implementation of ICT investment projects. International Journal of Production Economics, 80(1), 105-117.
[11] Pilat, D. D., Lee, F., & Van Ark, B. (2003). Production and use of ICT: A sectoral perspective on productivity growth in the OECD area. OECD Publishing.
[12] Petersen, M. A., &Rajan, R. G. (2002). Does distance still matter? The information revolution in small business lending. The journal of Finance, 57(6), 2533-2570.
[13] Reynolds, D., Treharne, D., & Tripp, H. (2003). ICT—the hopes and the reality. British journal of educational technology, 34(2), 151-167.
[14] Stiroh, K. J. (2002). Are ICT spillovers driving the New Economy? Review of Income and Wealth, 48(1), 33-57.
[15] Zuppo, C. M. (2012). Defining ICT in a boundary less world: The development of a working hierarchy. International Journal of Managing Information Technology, 4(3), 13.