**Thesis for the Degree of Master of Engineering**

# A study on the Business Process Redesign for Information Security Governance and Control of Kenya Banking System


**by**

**Bright Gameli Mawudor**

**Department of IT Convergence and Application Engineering**

**The Graduate School**

**Pukyong National University**

**August 2014**

# A study on the Business Process Redesign for Information Security Governance and Control of Kenya Banking System

# 케냐 뱅킹 시스템의 정보보호 거버넌스와 통제를 위한 비즈니스 프로세스의 재설계에 관한 연구

**Advisor: Prof. Man-Gon Park**

**by**

**Bright Gameli Mawudor**

**A thesis submitted in partial fulfillment of the requirements for the degree of**

**Master of Engineering**

**in the Department of IT Convergence and Application Engineering,**
**The Graduate School, Pukyong National University**

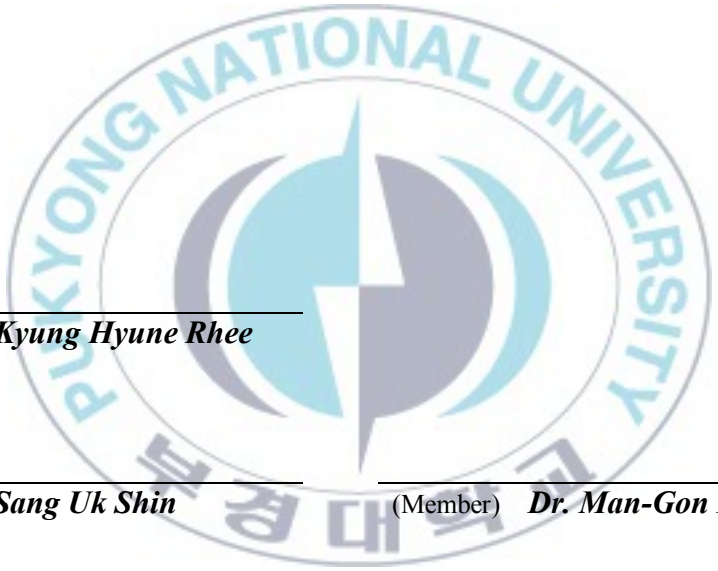
**August 2014**

**A study on the Business Process Redesign for Information Security Governance and Control of Kenya Banking System**

**A dissertation**

**by**

**Bright Gameli Mawudor**



Approved by:

(Chairman) ***Dr. Kyung Hyune Rhee***

(Member) ***Dr. Sang Uk Shin***

(Member) ***Dr. Man-Gon Park***

**August 31, 2014**

# CONTENTS

# List of Tables



# List of Figures

# 케냐 뱅킹 시스템의 정보보호 거버넌스와 통제를 위한 비즈니스 프로세스의 재설계에 관한 연구

**브라이트 가멜리 마우도르(Bright Gameli Mawudor)**

**부경대학교 일반대학원 IT융합응용공학과**

## 요 약

빠른 기술 변화에 따라 케냐의 공공산업에서 정보 보안 문제가 주요 이슈가 되었다. 많은 컨퍼런스에서 보여주고 있는 기술 허브의 성장은 증가되고 있는 기술에 대한 관심을 보여주고 있다. 2009 년 도입된 4 개의 해저 케이블(TEAM, EASSy , SEACOM, LION-2)은 국가의 4 천만 사람들간의 연결을 증가시켰고 인터넷을 통해 정보에 접근하는 비용도 감소시켰다. 한편으로 케냐에서는 모바일 네트워크 운영사 사파리콤(Safaricom)에 의해 M-PESA 라 불리는 모바일 머니(Money)를 지불하는 혁신적인 솔루션이 도입되었고, 이는 뱅킹 산업을 중심으로 관련된 많은 혁신을 주도하고 있다. M-PESA 는 모바일 폰에서 다른 모바일 폰으로 돈을 전송할 수 있도록 하며, 또한 은행 계좌로의 입출금과 클라우드 기반의 많은 다른 플랫폼으로 전송도 가능하도록 하고 있다. 위의 사실에서 보면, 비즈니스 세계가 종이 파일, 물리적 머니, 파일 캐비닛으로부터 보안이 정교한 컴퓨터에 저장될 수 있는 전자 파일로 이동하고 있는 것을 보여주고 있다. 이런 패러다임 변화는 또한 전 세계에 문제점을 제기한다는 것을 인식하게 되었다. 최근에는 증가하는 정보 위험들로 이어지는 경쟁 이면에는 알지 못했던 문제점들 – 빅 데이터(Big Data)를 어디에 보관해야 하는지 그리고 어떻게 적절하게 관리해야 하는지 - 에 직면하였다. 케냐에서의 정보 위험들은 비공개 또는 기밀 전자 정보가 권한이 없는 자에 의해서 접근되거나 악용될 수 있다는 것이다. 많은 은행 조직들이 그들의 민감한 데이터에 대한 무단 접근과 변경을 당하는 보안침해와 데이터 손실을 경험하고 있다. 이는 케냐 정보 기술 사회에서의 커다란 손실이며 정보 위험의 핵심 키이다. 네트워크를 침해하기 위한 해커들이 사용하는 방법은 진화되고 있고 기능적으로 정교해지고 있다. 따라서 오늘날 사이버 공격에 대한 부정적인 영향은 이런 프로세스에서 잃을 수 있는 수익과 신뢰의 손실 때문에 가볍게 다룰 수 없다. 비즈니스 연속성이 항상 은행과 모든 조직에서 우선순위였지만 갈수록 정보 보안이 우선순위가 되고 있다.

본 논문에서는 케냐 뱅킹 시스템의 문제를 해결하기 위한 프레임워크를 제안하였다. 이를 위해 사이버 보안과 관련된 케냐의 주요 기관 2 군데의 보고서를 분석하였다. 첫 번째는 기업 위험에 대한 보안관리와 컨설팅을 위한 국제 기관인 Deloitte Touche Tohmatsu 에 의해 작성된 보고서로서 2011 년 동아프리카 조직 전체의 사이버 보안 위협에 대해 작성되었다. 이 보고서는 동 아프리카 시장에 대한 일반적인 관점의 정보 보안 문제에 대해 이해할 수 있도록 작성되었으며, 본 논문에서는 금융 부문에 초점을 맞추어 분석하였다. 두 번째는 2012 년 케냐의 정보 보안 컨설팅 회사인 Serianu 에 의해 작성된 보고서로서 동기와 방법론의 관점에서 케냐의 정보 보안 위협에 대해 작성되었다. 이 보고서는 케냐 사이버 공간에 초점을 맞추어 상세히 설명되어 있다. 2 개의 보고서 분석은 케냐 뱅킹 시스템의 사기와 사이버 공격으로 인한 손실의 원인을 찾아내고 격차를 없앨 수 있는 프레임워크를 도출하는 기초자료로서, 본 논문에서는 해커나 사이버 범죄에서 사용되는 새로운 방법들을 이해하고 문제를 해결하는데 필요한 프레임워크를 제안하였다.

# Chapter 1

# Introduction

## 1.1 Background

Kenya has 44 banks that are operating at different levels on a daily basis trying to increase the number of customers and also the amount of revenue or better understanding, want to have a good return on investments. However, it has been estimated by the Central bank of Kenya that commercial banks loose to fraudsters about Sh100 million on an average scale, monthly [1].This clearly shows how much risk is there to the financial sector through fraud in Kenya.

A better way to define this is as a result of threats, defined as a possibility for a source to successfully carry out a particular vulnerability and "a vulnerability is a weakness that can be accidentally triggered or intentionally exploited"[3]. The tools and skills that are there to commit these crimes are getting easily acquired through the internet and also the usage does not take one that much effort to get around. A tech savvy simply doing a Google search will produce numerous results to enable one learn in a few minutes and practice on existing vulnerable systems. The probability that one may abuse these and thus have an impact on the bank business as a whole becomes the risk.

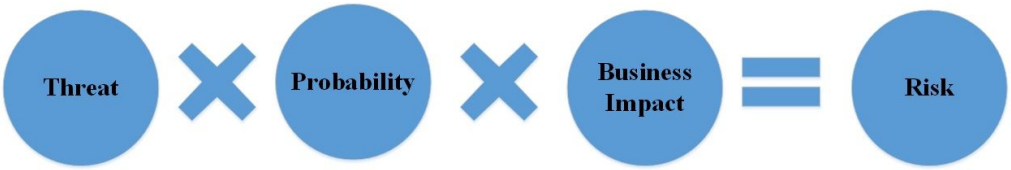



Figure 1.1 A Definition of Risk as a Result of Threat, Probability and Business Impact

Central Bank of Kenya (CBK), fraud department indicated that the reported incidence of

banking fraud rose from 0.5% to 3% in just 5years [1]. This has been due to not just the skill set of individuals but also the advanced technology advancements that are being used inside the banks and the fast internet connectivity. In addition to the technology side of things, the human element and governance are also a contribution. Disgruntled employees help in carrying out criminal acts for various reasons they might have to colleagues that they work with, customers or the bank as a whole.

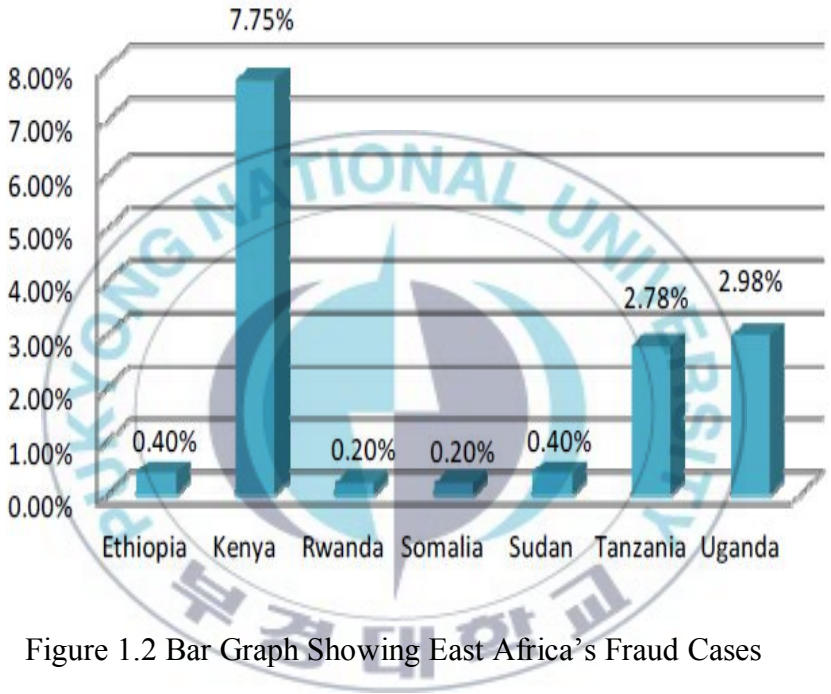



Figure 1.2 Bar Graph Showing East Africa's Fraud Cases

A survey done by KPMG International in 2012 indicates in **Figure 1.2** that Kenya has the highest occurrences of fraud incidences in East Africa. Such reports emphasizes the severity of the fraud in the entire country and not just the financial sector or to be specific the banking sector

## 1.2 Purpose and Structure of the Thesis

In this thesis, we aim at to try and understand the nature of the present environment in the Kenyan cyber space ranging from past record. This will enable us to be able to analyze the common or related problems and predict better future solutions. We will also diverge

slightly to analyze a few data and trends from the East African Information Technology environment with special attention to Information Security. Such an approach will help to realize the different methodologies that are being adopted or applied. Another aim of this thesis is to try and dive deeper into the real problems that is making the Kenyan banks lose so much money to fraud and cybercrime. The knowledge from the study will help in giving the utmost and necessary mitigations to help curb or eradicate these problems as much as possible. Having known all that, a framework will be developed to help the Kenyan banking industry tackle their issues pertaining to information technology and especially security as a whole. The framework that we will come up with will be based from ideas gleaned from previous successful study in information security across the globe and then revamp with extensions to meet the requirements and expectations of the problems found in the Kenyan banking structure. We will be using BPWin Fusion Modeler for the development as it has proven worldwide of its capabilities to elaborate a structure smoothly and easily understandable by anyone. Regardless of the details of the study, the general focus will be the blending of both business and technical aspects of a Kenyan bank to secure all loopholes as this has been known to be the trend across the world.

The structure of this thesis is broken down into the following modules:

***Chapter 1*** Introduces the facts and figures of the state of information security in the Kenyan IT world in defining the risks.

***Chapter 2*** Examines the real problems that are being faced in the industry by looking in depth of previous works studied by experts in the field from Serianu Cyber team and Delloite International in Kenya.

***Chapter 3*** discusses the evolution of malware and botnets actions that could be affecting the external facing infrastructures of the banks.

***Chapter 4*** recommends the building blocks of a framework that can be used to solve these security issues that the industry is facing by focusing on the application development practices and business sides.

***Chapter 5*** is the mitigations in the framework that has been arrived at from all the analysis.

***Chapter 6 c***oncludes the thesis and seeks to see how future research could be carried out

# Chapter 2

# Understanding the Information Security Practices in the Kenyan Banking Industry

## 2.1 Scrutinizing the Main Problems

Every banks and most corporate seek to advance in their organization by always introducing new technologies and practices to be at a level of the competing market. A typical mindset and mistake that most make is not following the right path when reviewing these methodologies. For example, a new banking software being introduced into the banking sector is not tested or vetted properly before deployment thus leave a lot of security holes in the application with a lot of vulnerabilities. Details about such security openings will be explained later in this paper.

> *Gartner stated: "Over 70% of security vulnerabilities exist at the application layer, not the network layer."* [2]

Most deployed applications in the banks are done in haste so much that the vulnerabilities are easily exploited without a trace. The contracted software developing companies or in-house development teams are usually rushed to complete an application and integrate within a short period thus leaving unfinished sectors. Secure coding practices are part solutions that are always avoided and needs to be incorporated into a banks technological consideration. Be it that they developing applications in-house or outsourcing the service.

The theft in Kenya does not just range from the fraud inside the banks but also "Card theft, information skimming (insertion of electronic devices in ATM machines to capture customers' personal data), compromised PINs and vandalism [1].

The percentage of incidents rose from 0.5% to 3% in just five years which might be

due to the introduction of the fiber connectivity and also the level high usage of technology in the banks according to CBK's fraud department [1].

Kenya is not known for high usage of credit card as a payment method but with the upcoming integration of the e-commerce portals, that is a growing area. This element directs the target to shift from physical attacks of e.g. ATM to online cyber-attacks. About Ksh20 billion has been invested in this sector to safeguard customers from such attacks [1].

## 2.2 Analysis of Previous Information Security Reports

Now that we know the background of the nature of banking and security environment in the Kenyan space, it will be good to understand the various reports that has been released to be able to come up with a good framework and mitigations. One that will be able to address all sectors of the information security problems affecting the Kenyan banks and businesses are a whole. The main point of concern is clearly making out the main issues.



### 2.2.1 Delloite Report

Delloite is a well-known and respectable organization when it comes to governance and Enterprise risk internationally. The branch in Nairobi, Kenya did a research back in 2011 dubbed "East Africa Security Study Report, Protecting what matters."

Taking into consideration that as an organization grows, information security is being drilled down to be business oriented and worked around information risk management. However, presently, it is changing from just the technological side to a more business focused type.

The studies main aim is to determine in relation to Information Security threats, how the East African businesses are planning, improving and doing a maintenance against them. This

will help them to be able to know what is happening in the information security environment of security personnel and their organization by using web-based surveys.

The targeted survey audience included technology, financial and general businesses across East Africa ranging from technical to governance implementations and analysis. What we like about this report is that it does not only try to understand the present information security problem these organizations face but also future schemes to be implemented.

The survey questions where grouped into the following categories:

(1) **Governance and Organization:**

Governance, Information Security Executive, Maturity, Developments in Information Security

(2) **Strategy, Business alignment & Metrics:**

Information Security Staffing, Investment, Reporting and Metrics

(3) **Operations, Emerging Trends & Outsourcing:**

Outsourcing and Third parties, Cyber Crime, Training and Awareness, Security Operations Center, Breaches, Security Technologies, Mobile Devices, Cloud Computing

(4) **Risk, Compliance and Privacy:**

Privacy, Regulatory Compliance, Global Systemic Risk, Threat Landscape, Audits

(5) **Global Systemic Risk and Cybercrime:**

Cyber intelligence, Critical infrastructure

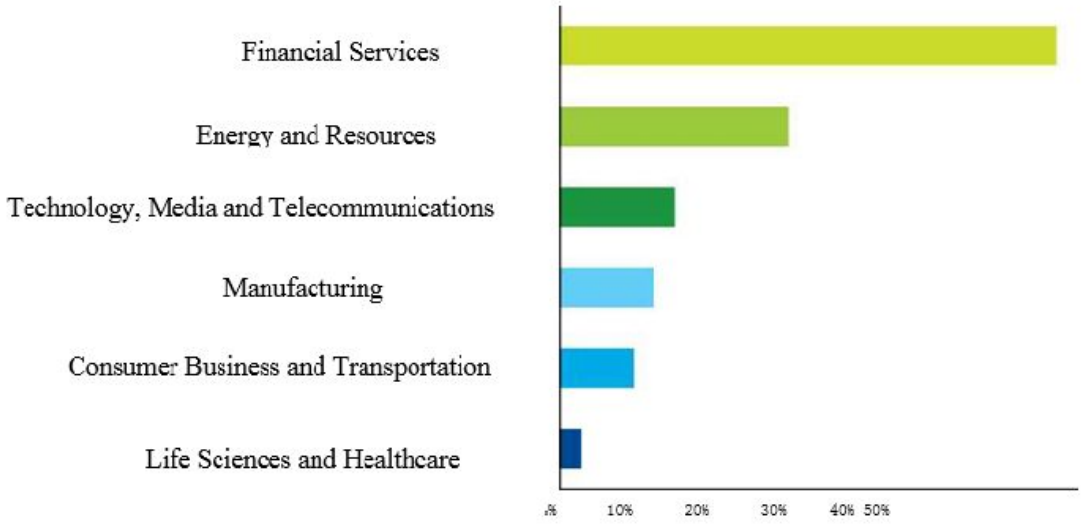



Figure 2.1 Industry Breakdown of the Survey

The **Figure 2.1** above illustrates the industry that responded during the survey. The financial services industry was the most which not only involve banks but insurance and micro finance among others. With such indication, one can tell that they did take it seriously enough to correspond.

Further information about the industry targeted for survey is below

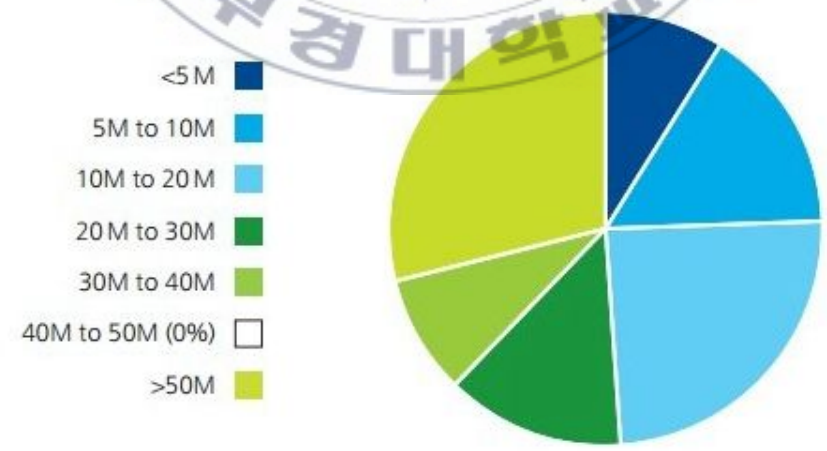



Figure 2.2 Annual Revenue 2010 in Million USD

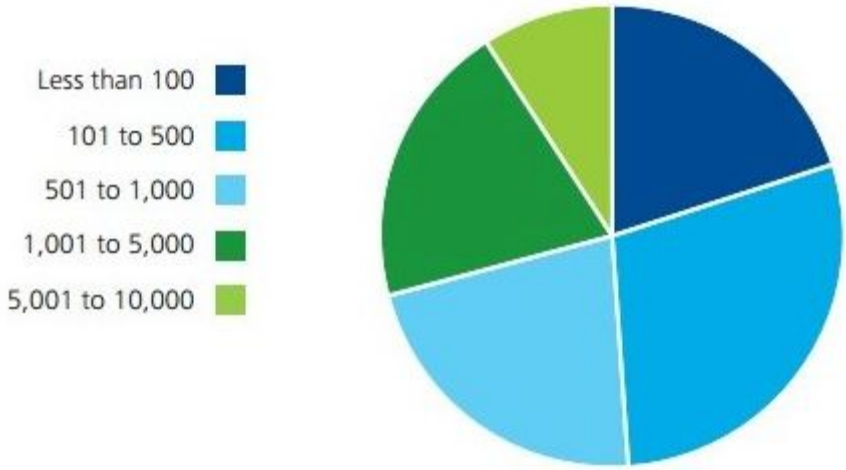



Figure 2.3 Number of Employees

The outcome of that study shows that majority of these organizations surveyed do not have the right capabilities to respond to a cyber-threat, on the basis of detection, prevention and investigation. They lack the right skills, have low budget for that sector of the business and worse visibility within the organization is not vivid. So many loopholes can be noticed here should a simple targeted attack let alone a persistent threat attack hit such organization. The top management not factoring information security into their annual budget leaves out good training for the stuff, then goes down to getting the right tools for detection and prevention for visibility in the organization. That creates a ripple effect as a threat will not be dealt with appropriately.

Dr. Anton Chuvakin, an IT security analyst mentioned in a report that:

*"...prevention and preventative security controls will fail. Prevention fails on a daily basis at many organizations; it will suffice to look at antivirus tools and contrast their 99%-plus deployment rates with widespread ongoing malware infection rates"* [4].

The comment by Dr. Anton seeks to be that the preventive method of security alone will not work for an organization and focus in this case Kenyan banks. Deployment of anti-viruses and firewalls alone is what most people understand to solve cyber security threats but it has to go way beyond that. Delloite suggested that financial services need to have strong information security programs that will include "skilled security workforce" who needs to be constantly trained to keep

up with the latest cyber threat methods. They go on to emphasize on the fact that the Security Operation Centers (SOCs) should be strengthened by deploying real-time monitoring technologies, such Security Information and Event Management (SIEM) and Data Loss Prevention (DLP).

Some of the key results and pointers discussed are listed below:

(1) Insiders present a bigger security threat compared to outsiders for East African organizations

(2) Security professionals are struggling to demonstrate business value to senior management

(3) Organizations do not have an authoritative source of information to make enterprise security decisions

(4) East African organizations lag in needed Employee Security Training & Awareness

(5) Most organizations have not implemented formal third party security assessment programs

(6) Cloud computing creates significant risks for East African Organizations

(7) Governments in the region have a critical role to play in ensuring information security

All the above have been confirmed in numerous graphical representations that confirms that indeed, Information Security is a very big problem in East African companies and needs to find a solution one way or the other. [5]

### (1) Information Security Function Size

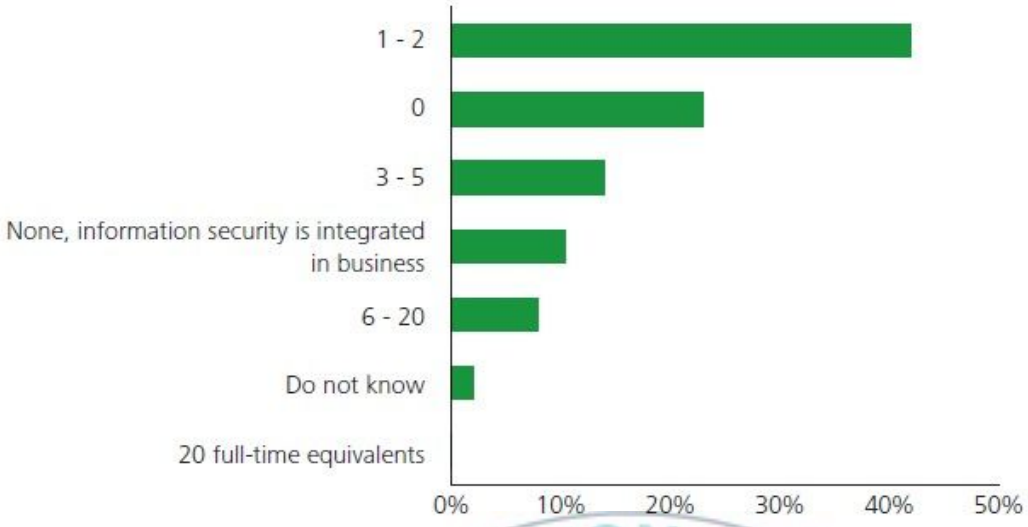



Figure 2.4 Number of Dedicated Information Security Officers

### (2) Information Security Strategy

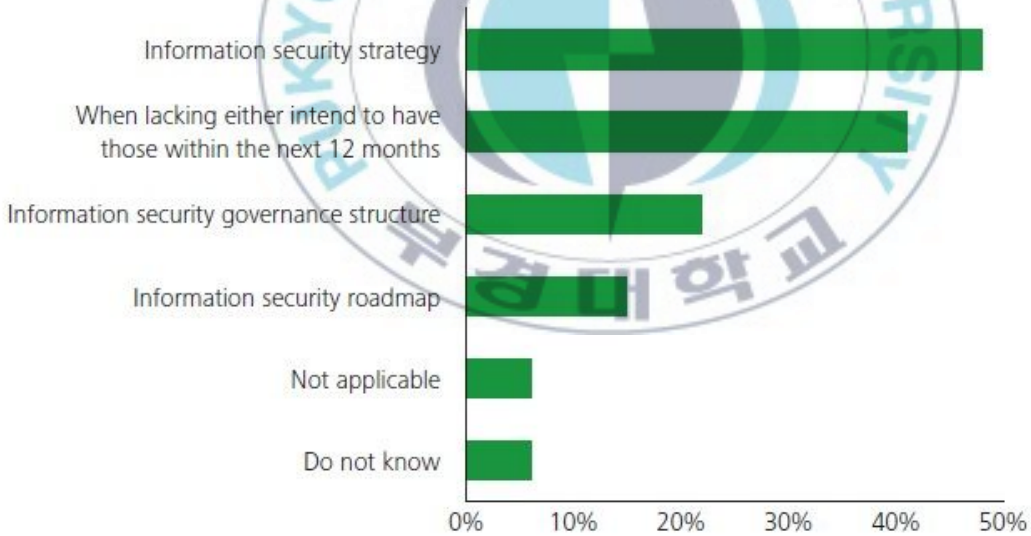



Figure 2.5 Presence of Defined Information Security Strategy

**(3) Alignment of Information Security and Business Initiatives**

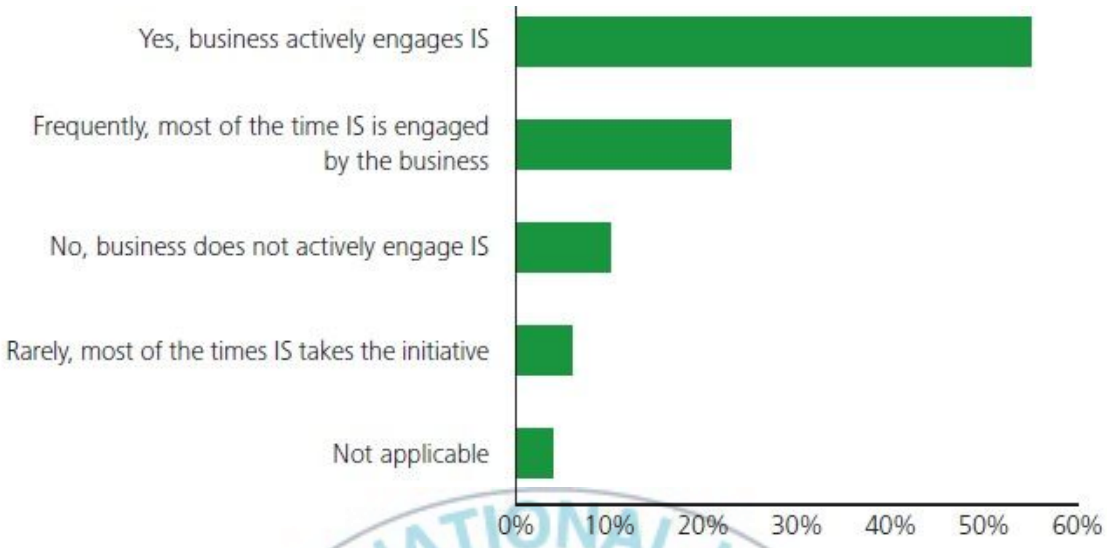



Figure 2.6 Level of Involvement of Information Security in Supporting Other Business Functions

**Figure 2.2, 2.3, 2.4, 2.5, 2.6** gives an overall overview of the state of information security covering East Africa focusing on the seriousness that originations take it to be when running their businesses or institutions.

### 2.2.2 Serianu Report

A little bit more focused view on the general trend of Cyber security in Kenya will be easy to understand from the Serianu Kenya Cyber Security Report. The report was aimed at trying to understand the "motives and methods of information security threats in Kenya. It covers all aspects that will make one understand at a glance what the situation in the Kenya internet cloud pertaining to Information security.

The report reveals that according to Communication Commission of Kenya (CCK), "there were an estimated 17.38 million internet users in Kenya as at December 2011. This represents a 95.63% increase from 8.8 million internet users reported in December 2010" [6].

Noticing the growth in the number of internet users makes a mark in a wider threat landscape. More attacks will be expected and a lot of cyber criminals, for whatever reason they want to carry out an attack, will usually need a large target space for good results. For example, in case of a bank, a targeted or advance persistent attack will require a lot of employees who work in the bank to probably open a link. Some might be security aware whilst others will fall for a scam with commonest known to be spear phishing attacks [7].

Further results from the reports indicate that the attacks locally in organizations have been in existence for a long time and not anything new. This begs the question of why are such occurrences, some more over embarrassing keep repeating without being detected or stopped having when the "experience" is there. Serianu view is, the fact that it is due to "poorly trained technical staff, misconfigured systems, lack of company security strategies and unpatched and vulnerable systems" [6]. Other major pointers picked from the 2012 report to better understand the Cyber security situation in Kenya include:

(1) Spamming, Phishing and poor reputation scores from the Internet service providers.

(2) A high number of Malware threats with viruses, Trojans, worms and botnets infecting a lot of machines and insecure web application leave loopholes to attacks to use to their advantage.

(3) Organizations in Kenya are being hit with automated attacks which go undetected for a long time due to poor detection and prevention methods. Moreover, the credit card fraud is getting easier as cyber criminals are selling the cards in underground markets for as cheap as $10 US dollars.

One method by which machines are being infected or target space increasing is by the amount of spam or malicious content that runs across. About 150 sampled spamming IPs where dispersed

to Internet Service Providers in Kenya and below is the analysis drawn for a period from January to April 2012.

Table 2.1 Data from Publicly Available Database, Detected Spam in the First Four Months of 2012 from Project Honey Pot

| Name of ISP | Number of IP addresses identified in our analysis | Number of total spam events detected | Number of comment post spam | Number of IP address in the top 20 all-time spammers |
|---|---|---|---|---|
| ISP 1 | 50 | 66,321 | 5,410 | 8 |
| ISP 2 | 24 | 34,210 | 1 | 1 |
| ISP3 | 21 | 14,594 | 806 | 2 |
| ISP 4 | 16 | 10,517 | 0 | 1 |
| ISP 5 | 9 | 6,723 | 405 | 0 |
| ISP 6 | 6 | 5,527 | 0 | 0 |
| ISP 7 | 7 | 4,877 | 200 | 1 |
| ISP 8 | 5 | 4,779 | 0 | 0 |
| ISP 9 | 5 | 3,987 | 0 | 4 |
| ISP 10 | 2 | 1,090 | 0 | 0 |
| ISP 11 | 2 | 477 | 0 | 1 |
| ISP 12 | 1 | 371 | 0 | 1 |
| ISP 13 | 1 | 282 | 0 | 0 |
| ISP14 | 1 | 68 | 0 | 0 |
| **Total** | **150** | **153,823** | **6,822** | **19** |

The above table clearly shows that there is a lot bots and spams running in the countries internet systems that might never have been noticed [6].

# Chapter 3

# Latest Attack Vectors of the Banking Infrastructure

## 3.1 Malwares and Botnets

After seeing the greater part of East Africa internet loopholes in chapter 2 which mostly dealt with people factor and applications, another big problem we have dwells in malwares and botnets. In the present time of cyber security, attacks are taking different forms in order to be more effective. Stealth, control and time is key hence the spread of malwares using botnets across networks [8]. Financial institutions are easy targets as they are believed to have insurance and not really look into it or have a good method to response. Any vulnerability an attacker will see in a network or application, they will take advantage of it and exploit to the deepest level of the organization. Through the use of botnets, one does not have to do a lot of work as it is automated to carry out functions as they are malicious applications to "hijack" our machines or devices for deceitful purposes [9].

The botnet activity is alive and nothing new to the community as it might have been working to bypass certain vulnerabilities. A few of these could be seen with online banking pages that do not have virtual keyboards which in turns allows the botnet to capture keystrokes from the user as they type in their password on a page that has forms for input [10]. Furthermore, some online banking applications do not have a 2PG authentication which is a method by which a user will have a separate page for username and password authentication before redirected to the legitimate successful page [11]. About 33 banks where sampled in East Africa to evaluate the possible botnet penetration due to the name vulnerabilities that it is most affected.

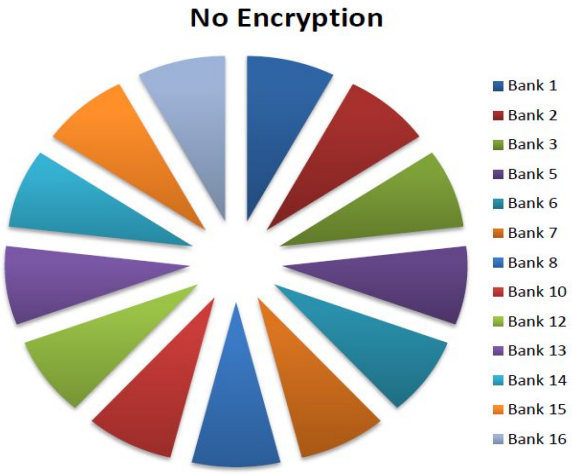



Figure 3.1 Banks with client side encryption - 2/33

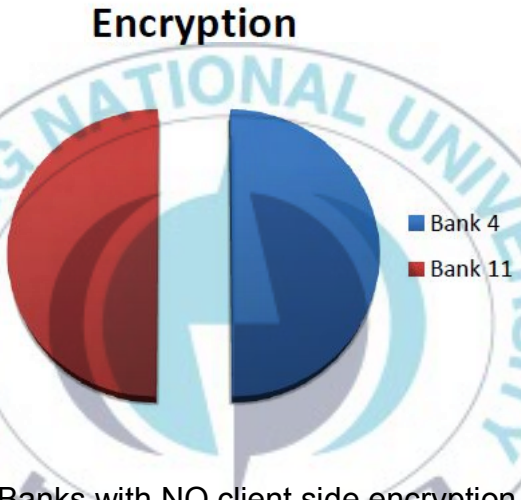



Figure 3.2 Banks with NO client side encryption - 31/33

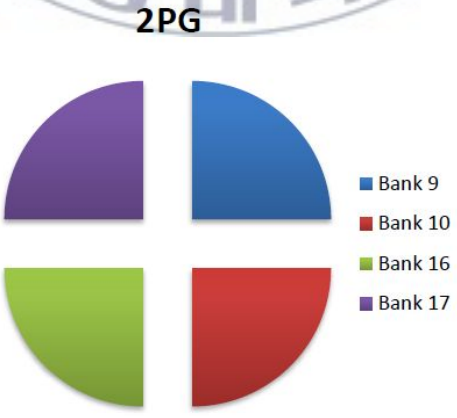



Figure 3.3 Banks using 2PG – 4/33

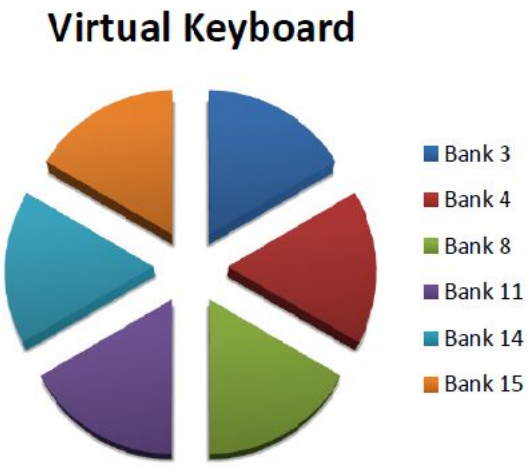



Figure 3.4 Banks using virtual keyboards – 6/33

Gathering from the various analyses of the reports, we can get two clear points of how banks in Kenya are losing money.

### 3.2 Root depth of a Malware or Botnet Effective Depth of the Malwares and Botnets

Present day hackers do like to not just get information but stay inside a targets network for a really long time. For this reason they aim to achieve a level of persistency where by the methodology used to infiltrate a system or network is carefully crafted or modelled to last for a long time. This is achieved by using easiest method as always thus the little loophole that an attacker sees open, he/she will utilize it. Analyzing the data from **Figure 3.1** and **Figure 3.2** indicates that only two banks out of the total thirty three sampled offer client side encryption meaning client side data storage is not encrypted. Client side storage is mostly user-specific data that is left on the system of the web user which is instigated by a web application but executed or controlled by the web browser or a plugin [12]. With the banks application in that state, very easy attacks are possible such as clickjacking or phishing where the interface could be manipulated for the user to think he/she is performing a particular operation whereas a non-legitimate action is being taken. Botnets actions are crafted well to retrieve all those sensitive information that is

being passed between the user and the bank since they are not encrypted and can effortlessly be read. This however occurs in the case of **Figure 3.3** for a 2-page authentication mechanism being implemented by only a few banks. It also allows for phishing to be carried out effortless and clients being the affected as they may fall into the wrong page and giving out sensitive data.

Furthermore, the statistics in **Figure 3.4** reports that only six banks use virtual keyboards on their web application. Virtual keyboards where designed to remediate keystrokes being captured by key loggers that might have infect a user who downloaded unwillingly through avenues such botnets yet again[10].

# Chapter 4
# Development of a Suitable Framework

## 4.1 Understanding the Applications and Loopholes

In this chapter, we want to be able to develop a framework that will give mitigation in favor of Kenyan banks to use when dealing with the affecting cyber security threats. These solutions will be drawn from various sources to come out with the best.

There is no bank currently in Kenya which uses a standalone application for operations of their system especially for internal network use. Nevertheless, they focus a lot of network firewalls, anti-viruses, and intrusion detection and prevention systems to secure the organization. However, these days' attacks are moving from network based to application based [13]. Our view over the years of interacting with experts in the Kenyan IT industry proves that majority of them are not really the sophisticated hackers as compared to other countries. There are activities of botnets and interesting traffic flow in the networks as gleaned by Serianu but there are no major attacks reported to other countries such as United States, United Kingdom etc.

The main problem is the applications being used internally have bugs thus can easily be manipulated without much skill needed. With the swift advancement of technology in Kenya, it will cost the banks a lot of money to hire permanent developers to take on a large project. For example, with the introduction of the M-PESA mobile money transfer system, banks had to be able to integrate the new industry system to work with theirs by allowing customers to send money to and from their bank accounts [14]. The development of such application will cost a lot of money thus they have to contract an outside organization do develop it.

Gartner statistic states:

*"If only 50 percent of software vulnerabilities were removed prior to production … costs would be reduced by 75 percent"* [2]

However, as much as these applications are being developed to make life easier and integrate into the banking systems, majority do not adhere to secure coding practices thus leaves the applications vulnerable to very easy attacks that doesn't require a skillful hacker to compromise. This is where the highest level of fraud takes place inside the banks as changes are being made without one noticing in their systems.

Microsoft Developer Research [15] is:

*"64% of developers are not confident in their ability to write secure applications."*

Apart from the internal manipulation, online banking is another entry point that money is being lost to the banks. The research from Serianu again shows that only 6 out of 33 sampled banks use virtual keyboards, 4 out of again the 33 banks use a 2-page authentication log in mechanism, 32 of the banks do not have a client side encryption. The above statistics proves that malwares such as client side or botnets will easily be able to work take over a system. Other types of attacks can be found from the OWASP TOP 10 webs which are listed below [11].

Table 4.1 OWASP Top 10 Most Dangerous Web Vulnerabilities

| | |
|---|---|
| A1 | Injection |
| A2 | Broken Authentication and Session Management (was formerly 2010-A3) |
| A3 | Cross-Site Scripting (XSS) (was formerly 2010-A2) |
| A4 | Insecure Direct Object References |
| A5 | Security Misconfiguration (was formerly 2010-A6) |
| A6 | Sensitive Data Exposure (2010-A7 Insecure Cryptographic Storage and 2010-A9 Insufficient Transport Layer Protection were merged to form 2013-A6) |

| | |
|---|---|
| A7 | Missing Function Level Access Control (renamed/broadened from 2010-A8 Failure to Restrict URL Access) |
| A8 | Cross-Site Request Forgery (CSRF) (was formerly 2010-A5) |
| A9 | Using Components with Known Vulnerabilities (new but was part of 2010-A6 – Security Misconfiguration) |
| A10 | Invalidated Redirects and Forwards |

## 4.2 Parallel Connection of Application Security to Corporate Governance

All technical solutions can be deployed but without the proper relationship to the business, it will not make sense or be of any level of use to the bank. Application security and governance has to be merged to be separate the wanted and unwanted needs in the bank. Secure software development processes has to be aligned with corporate policies and its activities with the compliance requirements to achieve best results.

A lot of applications are developed internally and even from contractors, it will be best to involve the management. Reason is that, most of the time the developers are focused on delivering to a specified time. Pressure to produce results tends to make the application become more usability centric to meet the revenue demands. Security then becomes an afterthought which at that point cannot be incorporated into the application as the result will break the flow of functionality when bugs are found and needed to be fixed. Involving top level management teams such risk management, legal and human resource can streamline the various right requirements needed for the application to be complete.

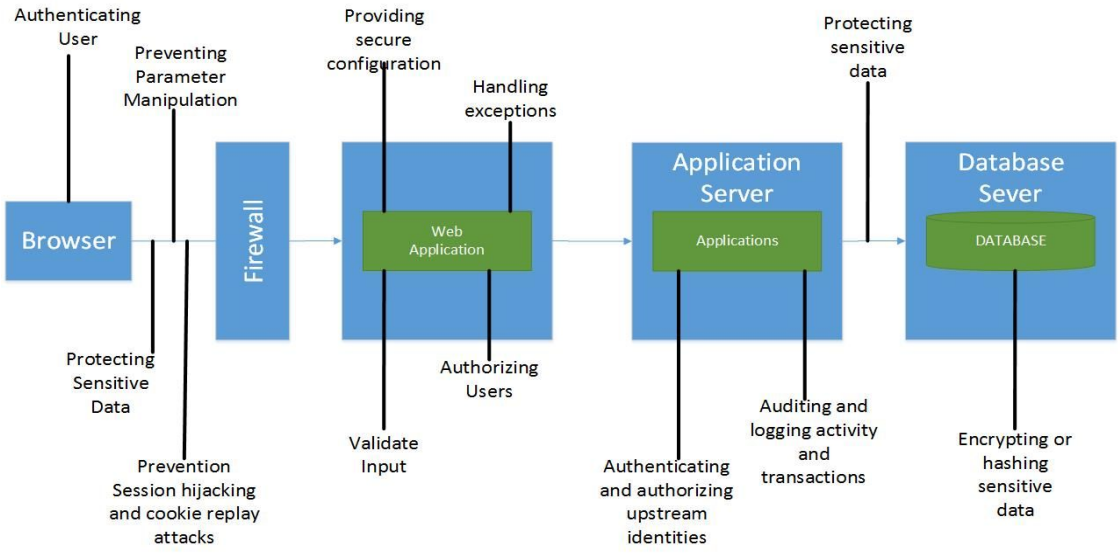



Figure 4.1 Representation of a Secure Web Application in a Secure Environment by Shaping Security

This does give a general overview of how a typical application should be deployed. However before the application is being created it has to go through a thorough review to lockout or minimize a lot of loopholes. The framework to be developed will be based on a methodology that is being used by Microsoft as their Software Development Lifecycle.

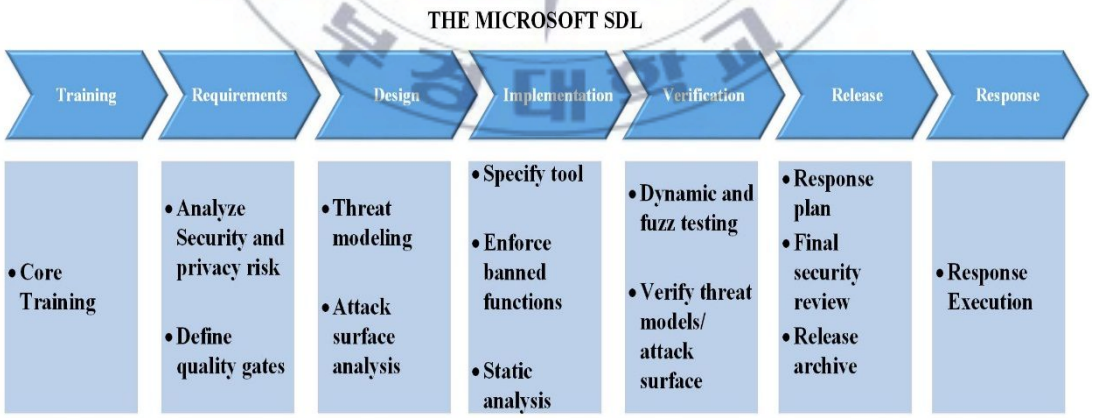



Figure 4.2 Microsoft Secure Software Development Lifecycle

To build on this a few modification has to be done that will suit the Kenyan banking industry. The main problem is the banks not being able to identify where the problem is when doing a post threat analysis of a breach or fraud case. To ask oneself, what are the main problems to

look for when targeting internal fraud or attack from an external source, the table below gives a summary for security at application and code levels.

Table 4.2 Security Hot Spots (Application Level)
by Shaping Software Limited

| Hot Spots | Examples |
|---|---|
| *Auditing and Logging* | ▪ User denies performing an operation.<br>▪ Attacker exploits an application without trace.<br>▪ Attacker covers his tracks. |
| *Authentication* | ▪ Network eavesdropping.<br>▪ Brute force attacks.<br>▪ Dictionary attacks.<br>▪ Cookie replay attacks.<br>▪ Credential theft. |
| *Authorization* | ▪ Elevation of privilege.<br>▪ Disclosure of confidential data.<br>▪ Data tampering.<br>▪ Luring attacks. |
| *configuration Management* | ▪ Unauthorized access to administration interfaces.<br>▪ Unauthorized access to configuration stores.<br>▪ Retrieval of clear text configuration secrets.<br>▪ Lack of individual accountability.<br>▪ Over-privileged process and service accounts. |
| *Cryptography* | ▪ Loss of decryption keys.<br>▪ Encryption cracking. |
| *Exception Management* | ▪ Revealing sensitive system or application details.<br>▪ Denial of service attacks. |
| *Input and Data Validation* | ▪ Buffer overflows.<br>▪ Cross-site scripting.<br>▪ SQL injection.<br>▪ Canonicalization attacks.<br>▪ Query string manipulation.<br>▪ Form field manipulation.<br>▪ Cookie manipulation.<br>▪ HTTP header manipulation. |
| *Sensitive Data* | ▪ Accessing sensitive data in storage.<br>▪ Accessing sensitive data in memory (including process dumps.)<br>▪ Network eavesdropping.<br>▪ Information disclosure. |
| *Session Management* | ▪ Session hijacking.<br>▪ Session replay.<br>▪ Man-in-the-middle attacks. |

Table 4.3 Security Hot Spots (Code Level) by Shaping Software Limited

| Hot Spots | Examples |
|---|---|
| *Authentication, Authorization and Trust* | ▪ Comparing Classes by Name<br>▪ Single-Factor Authentication<br>▪ Hard-coded Passwords |
| *Cryptography and Secrets* | ▪ Key Exchange Without Entity Authentication<br>▪ Failure to Add Integrity Check Value<br>▪ Failure to Follow Chain of Trust in Certificate Validation |
| *Language and Feature Misuse* | ▪ Failure to Protect Class Data with Assessors |
| *Logic Errors* | ▪ Improper Pointer Subtraction<br>▪ Failure to Deallocate Memory<br>▪ Assigning Instead of Comparing |
| *Memory* | ▪ Null Pointer Dereference<br>▪ Using Freed Memory<br>▪ Doubly Freeing Memory |
| *Range* | ▪ Buffer Overflow<br>▪ Stack Overflow<br>▪ Heap Overflow |
| *Synchronization and Timing* | ▪ Race Condition in Time of Check, Time of Use<br>▪ Unsafe Function Call from Signal Handler<br>▪ Passing Mutable Objects to an Untrusted Method |
| *Type* | ▪ Format String<br>▪ Truncation<br>▪ Sign Conversion |
| *Validation* | ▪ Cross-site Scripting<br>▪ Command Injection<br>▪ Deserialization of Untrusted Data |

## 4.3 Security of the Web Application Together with Compliance

The creation of the applications has to have security incorporated from design to deployment stages. Applying compliance standards such as PCI DSS will in turn reduce software development costs and also improve delivery schedules. The reason for such practice is that, should security be avoided at the beginning and placed at the end, fixing loopholes after a vulnerability assessment or

penetration testing will be tasking. Usability and functionality might need changes thus affecting the timeline for delivery and "go live" of the application. At such moments is when the top level management might understand and want the application to be deployed for use which in turn gets to be abused and makes the entire organization vulnerable to attacks and fraud [16]:

"*If only 50 percent of software vulnerabilities were removed prior to production … costs would be reduced by 75 percent*" [2]

# Chapter 5

# Suggested Mitigations to Kenya Banks for Information Security Revamp Framework

## 5.1 Governance, Risk and Compliance Standards

Certain decisions making has to come from the highest part of the bank executive structure and the earlier an information is relayed to them, the faster will they set the control mechanism to effectively manage critical information. Every bank in Kenya has governance as per requirements and it is a very wide and deep consideration that needs to be taken seriously. I believe prioritizing what information to be taken out will assist in risk management to eliminate the most critical threats in the banks and better yet, timely.

A lot of banks or financial institutions struggle to stay compliant to *Payment Card Industry (PCI)* -DSS and International Organization for Standardization (ISO) compliant, the most common known to be ISO 27001 and many other revised standards [16]. There is no record reporting any of the banks attaining such certification although there are clear signs that some parts of the compliances processes are being practiced. This conclusion has been my deductions from mere observation around the many banking sectors. Compliance standards acquisition can solve a lot of

security problems as majority of the rules and checklist are very strict when it comes to details.

## 5.2 Policy Implementation

However, when these policies lack thorough enforcement or implementation then it does not serve its purpose for being developed. Security policies in Kenyan banks has to not only be set up to execute, on after effects situations such incidences but rather should be applied at the beginning of the software development life cycle. All participating parties, such as Security, application developer, Quality assurance and audit teams needs to drill down all available policies from the very start of an application being developed to forensics being done by auditors when needed. Defects noticed early can be identified as security risks according to industry standard Common Weakness Enumeration (CWE). The CWE "provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design" [17] .Following such stands will not only improve security of applications for the bank but also the quality.

## 5.3 Other Mitigations to the Kenyan Banks for Information Security

The collection of all data and analysis from various sources made us to come up with these solutions that will help curb the insecurities in the Kenya banking sector. Sub chapters 5.1. [1-6] explains the mitigation processes and all has been backed up by the framework explained in **Figures 5. [1-6].** Conversely, it is a good preparation to have a threat modeling and attack surface reduction (e.g. Encrypted authentication, unauthorized access, Short Messaging Service (SMS) Authentication (2factor), Source code display, Session only and Timeouts, No cache,

Disable autocomplete, SSL encryption, Solid Input validation). Threat modeling is a semi-formal technique used to that can be used to understand the threat against your system [18]. Kenyan banks needs this when creating their web application so as not to miss any potential threat. Such practice helps one to identify security objectives, have an application overview by decomposing it and then check for possible failure points for solutions. The points below clarifies the mitigation:

- Remove entry points
- Check unwanted services and ports
- Remove entry points
- Identify threats and vulnerabilities to be expected at various levels of access(Application/Host/Network/Database)
- Vulnerability Assessment against OWASP TOP 10
- Secluded from database server and in a secure location

### 5.3.1 Continues Monitoring: Visibility of Infrastructure

Logs Aggregation and Security Incident and Event Management (SIEM) configuration forms the basis for visibility in a network. Implementing all security protocols and tools will not be effective is there is no visibility. Having a Security Incident and Event Management (SIEM) in the network to monitor the applications for anomalies can reduce security breaches [19]. The monitoring will be an aggregation of logs collected from the applications and network appliances. Custom rules have to be written for these logs for the administrators to be able to clearly and easily manage the bank. Such practice will in turn help that auditors and forensic engineers try to narrow down a breach or when doing a report. This can be in line with the policies that are meant to govern the bank. A typical example is an employee finding a way to install a remote application on his work desktop. This could be used by an outsider to connect to the internal network

and make transactions when the user is intentionally away from his machine.

### 5.3.2 Sharing Attack Information

Charts previously displayed in **Figure 3.1, 3.2, 3.3, and 3.4** illustrates the similarities of possible flaws in the Kenyan banking systems. However, most organizations do log like to share their breaches or information about how they got compromised with other banks for the fear of losing credibility. There is a body known as Kenya Banking Association, whose aim "was to cater for interests of the member banks in negotiating terms and conditions of service of its union sable employees and as far as possible, standardize management practices so as to ensure harmony in the Industry" [20]. Such can be medium to share details which will prevent others from being attacked. For example, if there is a malware spreading through Spearphising attacks or a zero day exploit for common applications being used by the banks, one bank sharing such information can save the others from repetition.

### 5.3.3 Perimeter Security

Network security is always considered as a first line of defense for any organization. Kenyan banks seems to have been doing well in this sector but precautions still have to be taken into consideration for more scrutiny. Firewalls, both Intrusion Detection and Prevention systems mostly have focus on inbound communication as known for their inbuilt signature. However, should an intruder be syphoning data out of the network, it also has to be looked at closely thus outbound traffic should be included in incident management views [21]. An extra layer of defense to the monitoring of outbound traffic for this will be implementing a Data Loss Prevention

(DLP) technology which will help the banks identify their sensitive data and better yet encrypt them [22].

### 5.3.4 Prioritization of High Risk Individuals

A lot of organizations get to be compromised not via sophisticated Layer 7 also known as the network layer attacks web attacks but just through spear phishing. Spear phishing is targeting specific personnel or people in an organization and compromising their machine or device to breach future into the networks. Banks in Kenya have to identify who are the high value targets that hold certain level of confidential information. This may include CEOs and Directors having documents meant for just a few, or worse it could be the heads of IT having passwords stored on their machine. Such personnel need more attention and extra vigilance and training on what to look out for when coming to terms with cyber space.

### 5.3.5 Red Teaming

This is a process to detect network and system vulnerabilities and also test security by simulating an attacker approach to system/network/data access [13]. It mostly involves hiring an external penetration tester, who has no idea about the network target or only has minimal knowledge beforehand to test the security from all angles. I believe Kenyan banks do need such testing in their yearly plans to be able to see all the loops holes that the internal security team might not be noticing due to having a big infrastructure or not knowledgeable enough.

### 5.3.6 Patch Management Structure

A known fact that runs with a lot banks is that, so far as a system is working they do not see the urge to ever tamper with it again. It is a bad practice that majority of them do not have a patch management implementation structure. This can be very detrimental to the systems as not only is there a higher level of the applications failing at a point but also easy to be exploited when an attacker gets to it [14]. New vulnerabilities will always be developed to beat the security of applications and systems as it is need for hackers to keep up with the software companies. There can be many points of failure for a system and thus a good patch management structure can make sure the banks systems are always up to date against the largely verifiable database of vulnerabilities. This is known as Common Vulnerabilities and Exposures (CVE), a standard for Information Security Vulnerability Names [23].

## 5.4 Suggested Framework Summary using All Fusion Modeler

In this section, it is appropriate to have an overviews of the activities involved in this framework with their various level of decomposition. This is illustrated with the HIPO chart below:

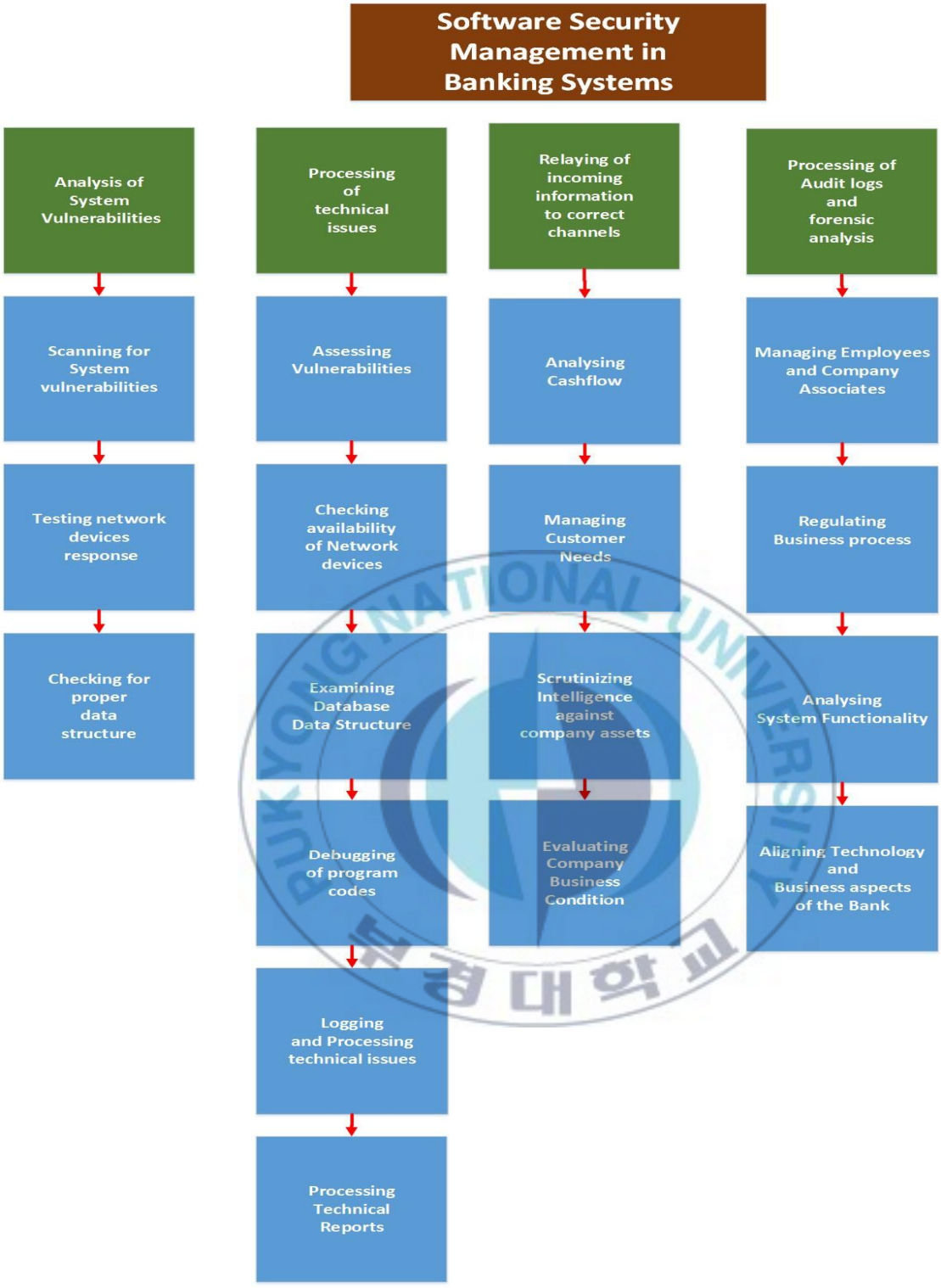



Figure 5.1 HIPO Chart of Software Security Management in Banking Systems

In this section I decided to put together a framework structure that can be used by the Kenyan banks to concentrate on the connection between the developers and governance. This is more of a

re-design of their business process from the analysis explained in the previous chapters. Using **BPWin All Fusion Modeler** [24], the business process using IDEF0 makes it easier for anyone to understand as each process can be decomposed into sub process. An IDEF0 diagram contains 4 types of arrows as follows:

(1) **Input:** something consumed in the process. Input border arrows can only be drawn from the left border to the left side of an activity.

(2) **Control:** A constraint on the operation of the process. Control border arrows can only be drawn from the top border to the top side of an activity.

(3) **Output:** Something that is a result of the process. Output border arrows can only be drawn from the right side of an activity to the right border.

(4) **Mechanism:** Something that is used to perform the process, but is not itself consumed. Mechanism border arrows can only be drawn from the bottom border to the bottom side of an activity [24].

The high level of this model is illustrated in **Figure 5.1** below in a context diagram

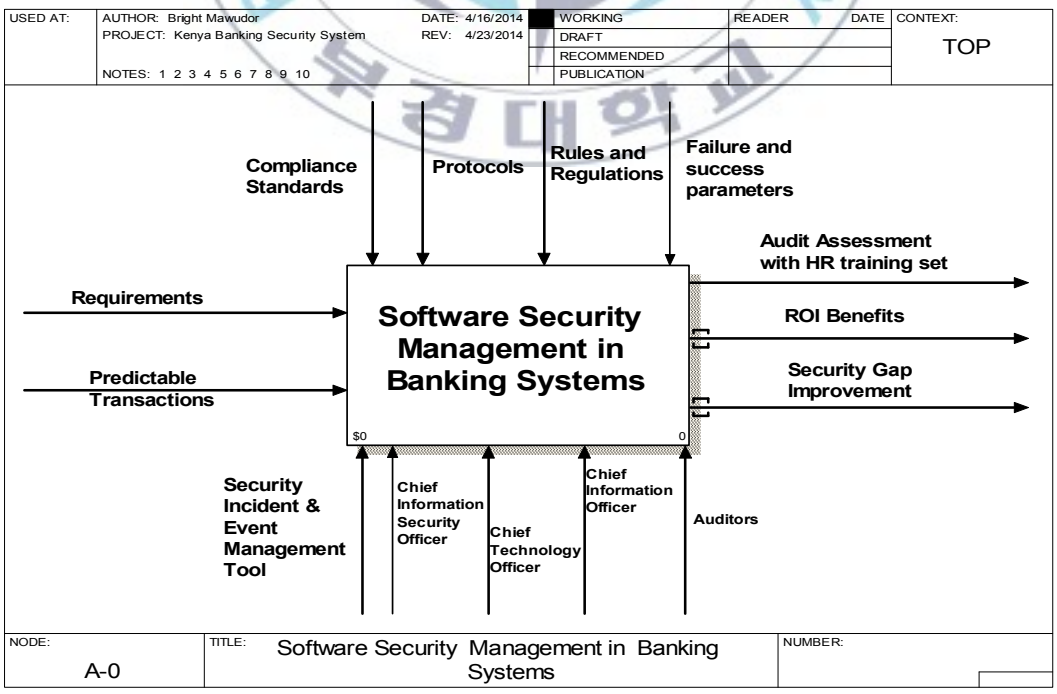



Figure 5.2 Context Diagram to Show the High Level Representation of the Model

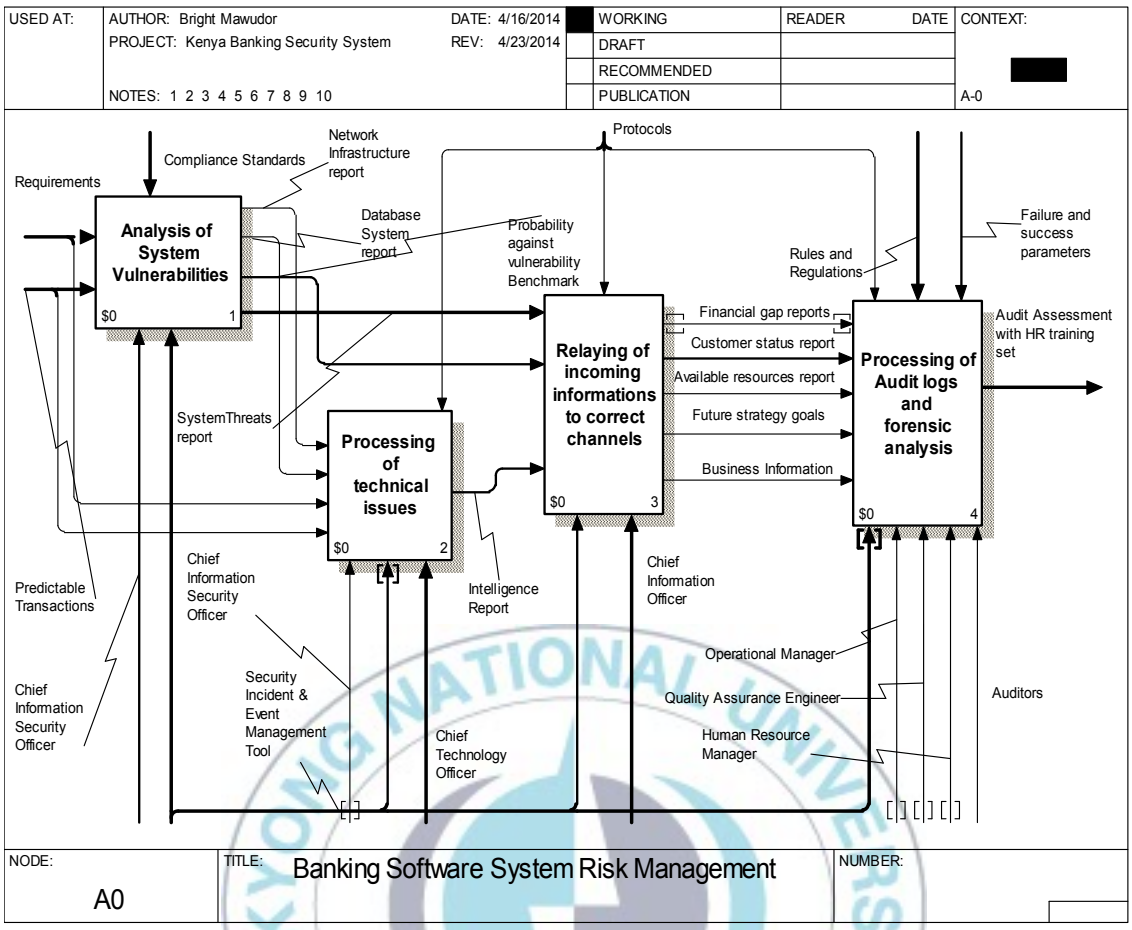



Figure 5.3 A0 Diagram Representing All Activities Involved in the Business Process

The A0 diagram shows all the activities involved to make this business process a success. The remediation proposal for Kenyan banking to connect the technical and business sectors will involve

- Information Security Management
- Technology Management
- Information Management
- Auditing and Assessment Team

An integration of all the above will be able to give the board of director a lucid understand of the banks needs and best methods to reduce risks.

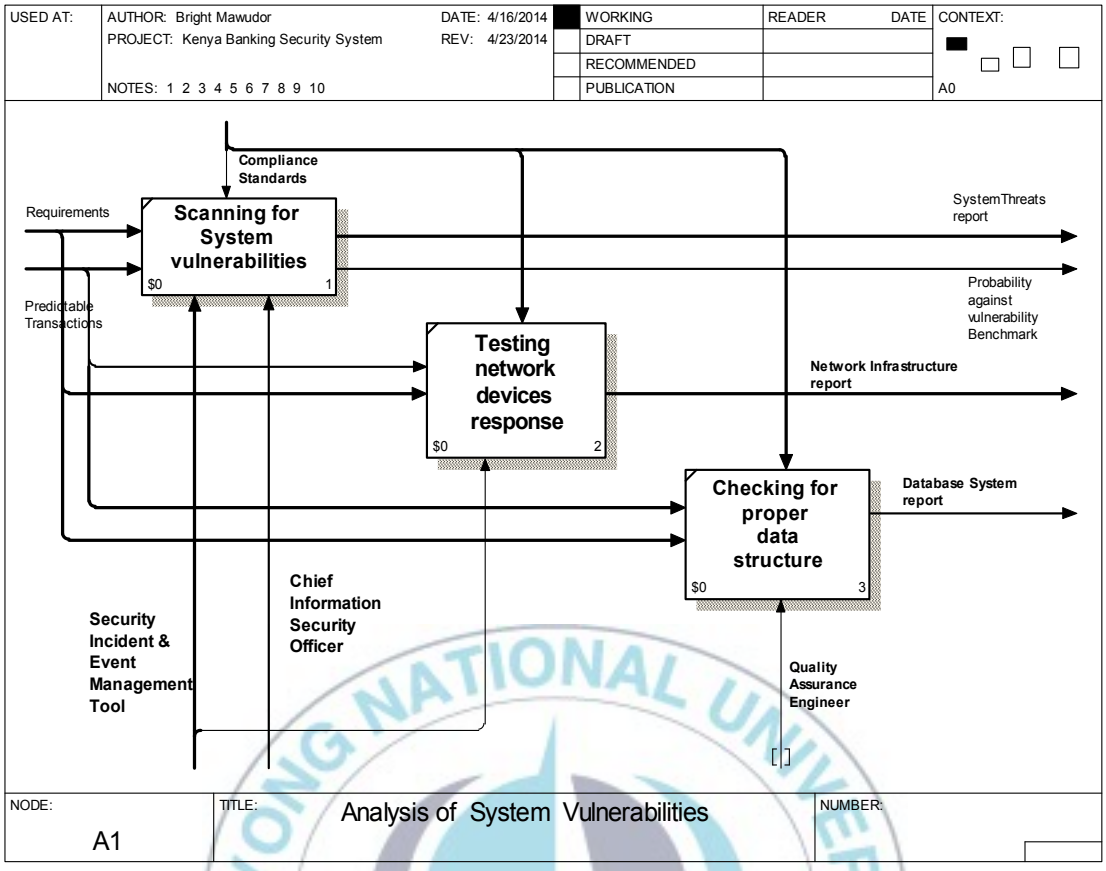



Figure 5.4 Information Security Management Position Decomposition

A good security revamp will start with the Chief Information Security Officer (CISO). The CISO function is to make sure all information assets and technologies are well secured as he has a general enterprise image and strategy of the bank. For that matter, **Figure 5.4** shows how he will be able to gather all requirements from the information security team, network administrator and database administrators whose final output will aid the next person in line to process well enough to identify general security risks in the banking organization.

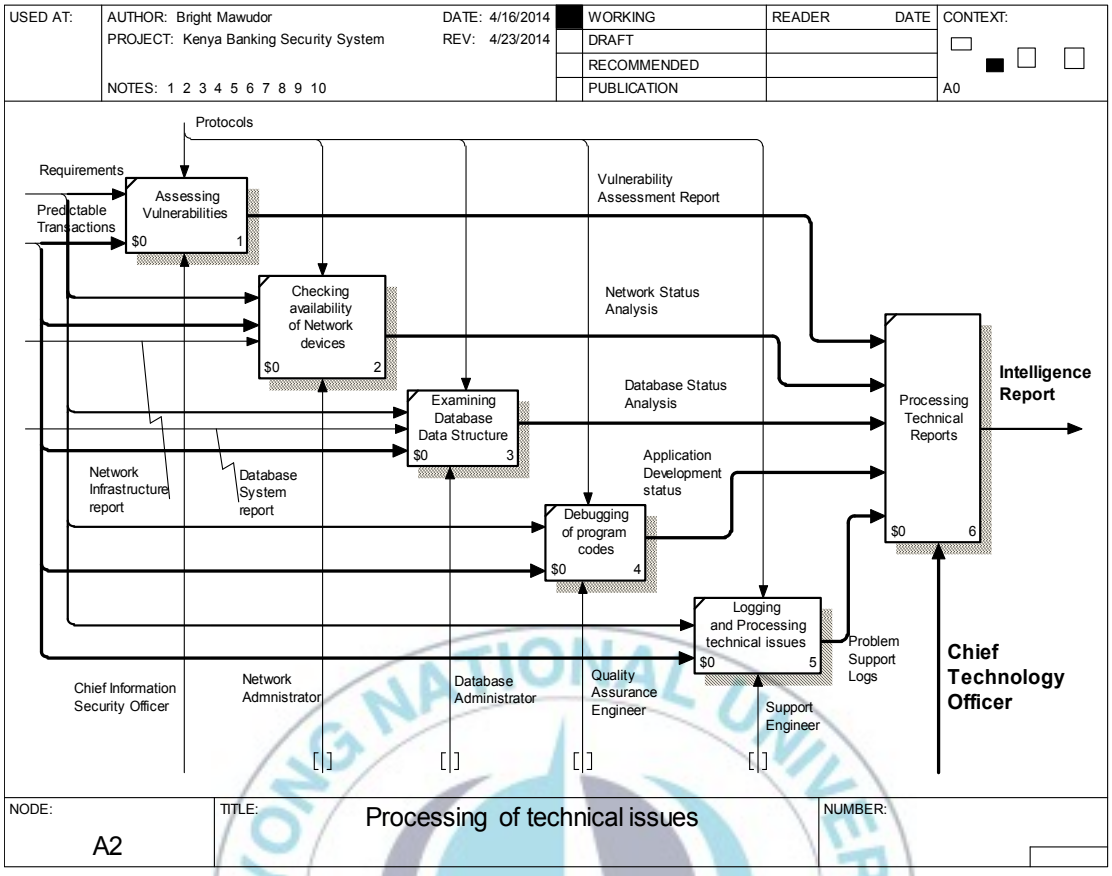



Figure5.5 Technology Management Decomposition in the Business Process of the Banking Systems

The Chief Technology officer (CTO) understands the impact of technology to the business in the sense that, he can measure the effectiveness using the same dimension that is used in business sector such as the Chief Executive Officer (CEO). For banks in Kenya using the process in **Figure 5.5** will enable all important data needed from the technology side be placed in a collective zone for proper analysis to the business. This is a very important part of the bridge to translate what the business sector of the bank do not understand from the technical division [25].

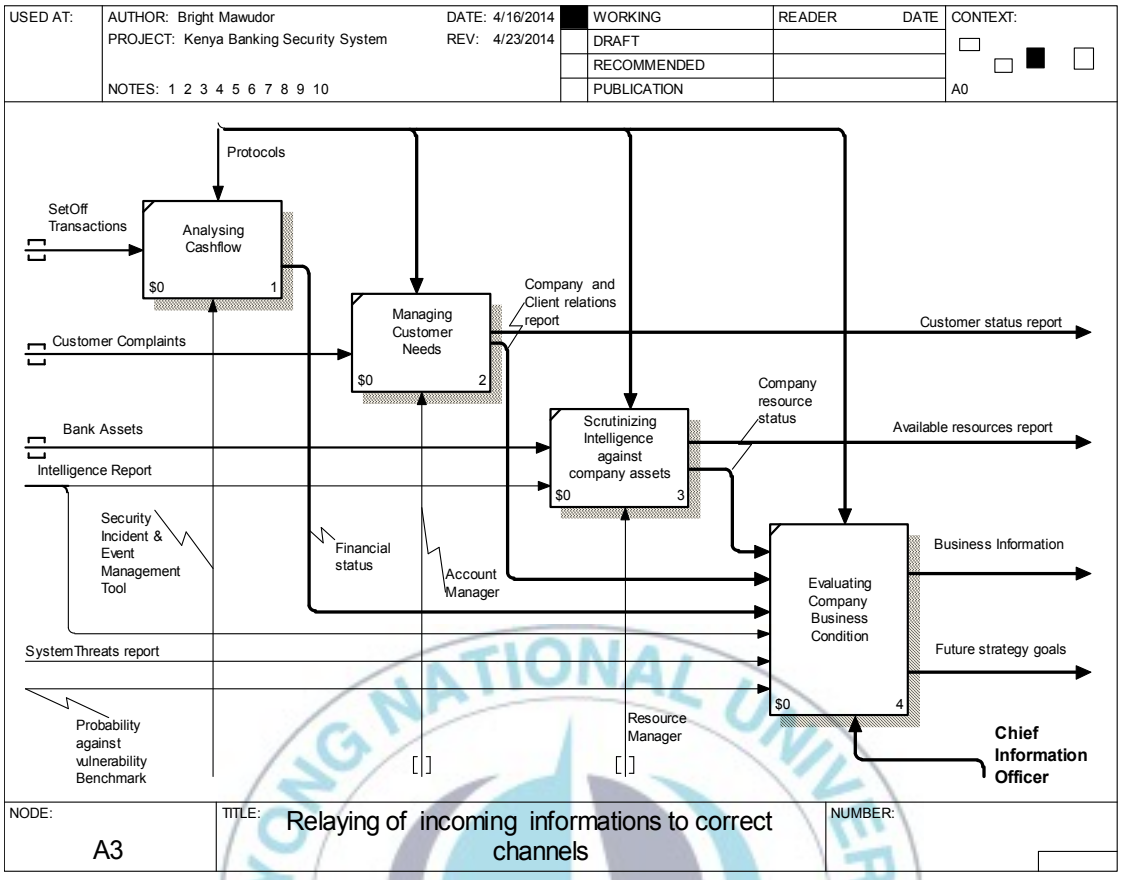



Figure 5.6 Information Management Representations in the Business Process

The personnel involved in this stage is the Chief Information Officer (CIO), who is mainly responsible for relaying of data across the entire organization. He also tries to show how Information technology can be used effectively to increase a return on investment for an organization. After collecting all information from the previous **Figure 5.4**, **Figure 5.5**, blending them with other sectors of the bank will make an efficient flow to determine the future changes to be made in the organization. This will involve the finance department analyzing cash flow, client account managers cordially interacting with various clientele, resource managers scrutinizing intelligence collected against company assets and finally the Chief information officer encompassing and evaluating company business condition to determine results such as future strategies [25].

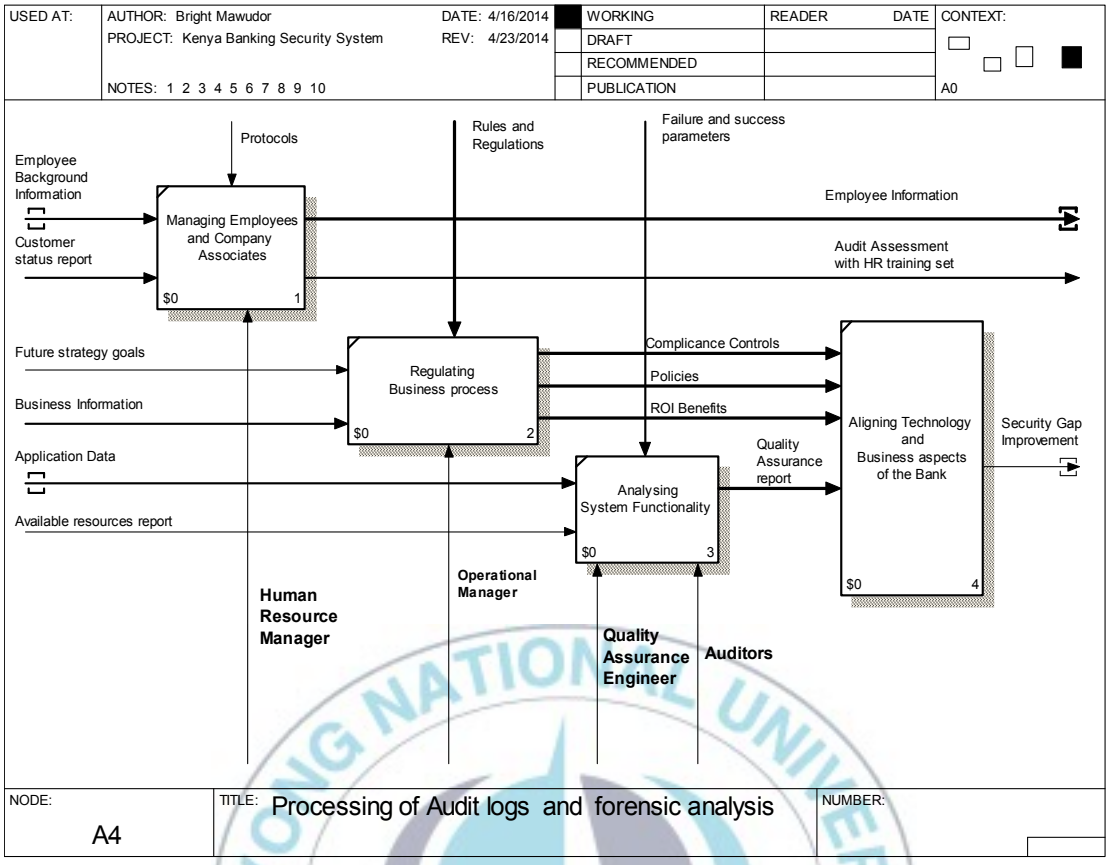



Figure 5.7 Auditing and Assessment Processing Stage of the Business Flow

This is the final stage of the business process that is suitable for Kenyan banks which is the Audit stage. The auditors will be able to carefully analyze all the information provided and quantify the risks involved, what needs to be changed to close the security gaps. Auditing gives a clear picture of what has been the misconnection between the technical security sector of the banks and the business.

However, final decision has to be made by the board of directors who most probably are not all tech savvy's but with such a business process model, some unclear questions such as

1. Why is the bank always losing money due to fraud or attacks?
2. Which sector/ branch of the bank needs a special attention or revamp?
3. What are the Return on Investments for the entire bank if certain technology is being implemented for security impact in the long run?

4. What future strategies need to be applied to eliminate or mitigate the identified risks in the entire banking?

# Chapter 6

# Conclusion and Further Discussions

Throughout my research into the minds, set ups and journeys of information security standards of the Kenyan banks, I will say it is one that will take a long time to fix. Business has to continue as usual without shake up or disruptions of operations so as to satisfy their esteemed customers. Also, there will be new changes to be made from time to due to technology changes influenced by demand and supply forces and it will only make forthcoming situation more complex if they do not implement the suggested security mitigation process.

Looking into the mitigations clearly, each and every one of them plays an important role to have minimized Information security incidents around the banks. Governance and compliance standards are very difficult to stand by or acquire in the banks as it involves a lot variables. If these protocols are followed or implemented very well, it will cut down a lot on Information security difficulties in the banks. Examples of such standards to take on are Payment Card Industry (PCI) Data Security Standard (DSS) and International Organization for Standardization (ISO) 27001-27002 which has been in existence for a long time but constantly being revised to fit changing environments. Another alleviation method suggested was policy implementation as a lot of banks create them but do not implement thus it is not effective. A change with such will bring a lot more benefit. Visibility of an infrastructure is always important to know what is coming into the network and what is leaving in terms of traffic and data. It is therefore important for the Kenyan banks, as much as they focusing also on applications security, do take into consideration close monitoring with the use of Security Incident and Event Management (SIEM) tools. Moreover, sharing attack information goes a long way to hasten the prevention of certain attacks. This is because if one or two banks have been attacked through a particular method or

vulnerability, there is a likelihood it will be repeated on others thus the need for attack information sharing. This can be done through the bodies such as Kenyan Bankers Association.

Another easy and common ways banks and other organization are being hacked is by social engineering top officials are they usually not security aware and should be considered high risk individuals. They need to be given extra attention in the area of information security to curb risks and incidents. Patch management and perimeter security go hand in hand as banks really do not have a set way to patch their systems at times where updates and upgrades get released. This mostly affects the perimeter security as it is always considered as the first line of defense. Finally, red teaming is a very important mitigation method as it allows an external penetration to try and get into the bank system and determine loopholes that will normally not be seen by the bank employees. It can help in reducing uncertainties as it will be a result viewing from a real attackers point.

Just like in any other organization, not necessarily a bank of financial institution, integrating new ideas, skills or methodologies is very difficult as it is a shift of cultural change. With regards to that, it will take a while for changes to be made and positive results realized in the face of security in the Kenyan banking industry. I believe it can be done if the write approach is being taken for implementation. One of the best approaches is that, the banks have to identify which undertakings are the most important to corporate governance priorities, after which they will be embraced in an order and later activate the others accordingly. The common methodology of "find it, fix it" will only last so long and can be very detrimental to the reputation and returns of the bank.

Furthermore, every business, not only in the banking sector are getting hyper extended. This means that, there are no more boundaries or perimeter to operation thus leaves a lot of openness. Kenyan banks will be dealing with outside contractors as "little" as cleaners who might not be considered as a big threat but that can be an easy route to infiltrating the network as they have

access.

Having looked at all sectors, the bottom line is that, top management level need to come to the same thinking states with technical staff members. The gap has to be closed to enable situations or incidences be reduced to the minimal level possible. Fraud from internal stuff, external breaches from hackers and internal attacks happening as employees are being used as a vector cannot be completely eradicated for a fact but can be curbed to a manageable standard [26].

In the future, I will however like to get access to more information from the banks that might have not been reflected in the already studied works and my thesis to come up with a more comprehensive framework and solution that will not only be used for Kenyan banks but also for East Africa and the world at large. Also, the recent announcement by Kenya Bankers Association for all banks to adopt “Europay, MasterCard and Visa” (EMV) chips and pin will definitely reduce fraud but more study in such an area will be highly regarded as it also does have possible loopholes as well [27] [28]. The information security state of Kenyan banks will sure get to level that will be appreciated but all in due time.

# References


[1] Kinyanjui K., “Banks fight to secure customer deposits from cyber criminals” *Business Daily Online*, Tuesday March 2,2010
Retrieved on 10th April 2014, from
http://www.businessdailyafrica.com/Corporate-News/-/539550/871390/-/14vf36iz/-/index.html

[2] Theresa Lanowitz, "Now Is the Time for Security at the Application Level".Gartner, ID Number: G001274071 December 2005.

[3] Stoneburner Gary, Goguen Alice, Feringa Alexis, “Risk Management Guide for Information Technology Systems”*NIST Special Publication 800-30*, pp. 12, July 2002.

[4] Gardiner M., “The critical incident response maturity journey” *EMC White Paper*, December 2013

[5] Nyang’aya J., Makatiani W., Okwiri F., Nchimbi D., "2011 East Africa Security Study Report" Protecting what matters, November 2011

[6] Serianu Cyber Intelligence Team., "Kenya Cyber Security Report 2012" *Getting Back to Security Basics EDITION ONE*, May 2012

[7] Allen L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, pp.3-36, 2012.

[8] Kapoor Aditya, Mathur Rachit, "Predicting The Future of Stealth Attacks” VIRUS BULLETIN CONFERENCE October 2011

[9] Instituto Nacional de Tecnologías de la Comunicación., “Silent threats on the Web: rootkits and botnets” December 2006.

[10] Parekh A., Pawar A., Munot P., Mantri P., “*Secure Authentication using Anti-Screenshot Virtual Keyboard*”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[11] MusuvaPaula, Kisutsa Christian, "The Advanced Malware Threats in Kenya's Cyberspace" AfricaHackon Conference, February 2014
Retrieved on Apr. 1, 2014 from http://africahackon.com/#contact

[12] Tump E., “*The Risks of Client-Side Data Storage*” SANS Institute Reading Room July, 2011.

[13] Peake C.,"*Red Teaming: The Art of Ethical Hacking*" GIAC Security Essentials Certification (GSEC) SANS Practical assignment Version 1.4b – Option 1, July 16, 2003.

[14] Suri T., Jack W., “The Economics of M-PESA: An Update” October 2010.

[15] Adams E.,"The Five Most Common Misconceptions of Enterprise Security" CIO Update, January 2007
Retrieved on Apr. 3, 2014 from
http://www.cioupdate.com/trends/article.php/3655891/The-Five-Most-Common-Misconceptions-of-Enterprise-Security.htm

[16] PCI Security Standards Council LLC., "*Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 2.0*" October 2010.

[17] Eric Bush. "A Gold Standard for Assessing the Coverage of Static Analyzers". 2013 IEEE International Conference on Technologies for Homeland Security. 2013-11 Ristic I. "Threat Modelling for Web Application Deployment" Thinking Stone, 2010.

[18] Butler M.J., "*Benchmarking Security Information Event Management (SIEM)*" pp. 9-11, 2009.

[19] Kenya Bankers Association Retrieved on Mar 2, 2014 from
http://www.kba.co.ke/overview/about-us

[20] Chickowski E., "*Perimeter Security*" Dark Reading Must Reads, June 30 2013
Retrieved on Oct. 7, 2013 from http://dc.tw.ubm-us.com/i/225519

[21] Park, Man-Gon., Mawudor Bright Gameli, "A Study on the Minimizing Advanced Persistent Threat (APT) Attacks", Korea Multimedia Society, 2013

[22] Neuhaus, S. Zimmermann, T., "Security Trend Analysis with CVE Topic Models". ISBN: 978-1-4244-9056-1, San Jose, CA, 1-4 Nov. 2010.

[23] Roger S."*Software Engineering (5th Edition)*" A Practitioner's Approach, McGraw Hill.

[24] Hart S. "Achieving Success as a CTO" Inside the Minds: C-Level executives, Aspatore Books, 2008.

[25] IBM Global Business Services, "Insights from the Global Chief Information Officer Study" The New Voice of the CIO, 2009.

[26] Soo-Mi Jang, Man-Gon Park, "A Study on the Fault Analysis and Security Assessment for Smart Card Management System," Journal of Korea Multimedia Society, Vol. 17, No. 1, pp.52-59, Jan. 2014.

[27] Myong-Hee Kim, Wildan Toyib, Man-Gon Park, "An Integrative Method of FTA and FMEA for Security Analysis of a Smart Phone," KIPS Trans. on Computer and Communication Systems, Vol. 2, No. 12, pp.541-552, Dec. 2014.

[28] Myong-Hee kim, Eun-Ji Jin, Man-Gon Park, "Fault Tree Analysis and Fault Modes and Effect Analysis forSecurity Evaluation of IC Card Payment Systems," Journal of Korea Multimedia Society, Vol. 16, No. 1, pp.87-99, Jan. 2013.

## Acknowledgement
## (감사의 말씀)

I want to first of all thank God for all the blessing and strength he has given me to go through this course to completing my Master thesis. It was not easy but it is a refreshing feeling to get to this point.

From the very first day I arrived in Busan, Rep of South Korea, I knew it would be a journey that I will never forget. A spectacular one for that matter undertakes my Master program at the Pukyong National University. Not forgetting the amazing culture shock that was bound to hit me as a foreigner, I was received warmly by Professor Man-Gon Park and former lab mate Kim dong-kyun.

This project wouldn't have been possible if not for the great support and guidance of my advisor Prof. Dr. Man-Gon Park. A great man, mentor, generous, wise and a father to me, even though away for the first one year of my education in his program, he was still supportive from afar in the United States on an exchange program. Studying under his supervision is one kind a blessing that not many are privileged to receive. From not only making sure I go through this course successfully but also lead me to attain publishing papers in Korean great books and taking part in conference. I will forever be grateful and owe it all to him for bringing a big change to my life as an academic and social person as a whole.

My family staying in Kenya, Ghana and United States has throughout been very supportive with constant calls and encouragement through all mediums as they know it is not easy to study abroad and as such being the first time to stay away for long. I cannot thank them enough for always helping out where they can from child birth to this high point of education. In addition, I would like to thank a friend and elder to me Tyrus Kamau, Chief Information Security Office for Cellulant group, Kenya, who saw a potential in me when pursuing my career to teach and guide me until I came for my Master program and also assisting in papers I published along the way. Not to forget a colleague Ivan Vincent Satoso, who assisted me when it came to a critical point of this thesis, which was the modeling of our framework.

An extended appreciation goes to Prof. Dr. Kyung-Hyne Rhee, Prof. Dr.Sang Uk Shin,

Prof. Dr. Yeon Ho Chung , Dr. Kim Myong-Hee , Dr. Hyun-Suk Hwang, Dr. Kim Su-Do, Dr. Kim Gyu-ah who have taught me in many disciplines ranging from cryptography, wireless networks, ubiquitous networks, internet technologies, JavaScript programming and cloud computing security. All the knowledge gleaned from the above great mentors is one that I will carry on forever in my future endeavors so once again thank you very much.

Finally I will like to say a special thank you to my lab mates and colleagues who had helped me in so many ways especially during my most confusing moments around the university. There were times I get so clueless on what to about a situation but they have always been there to make my life in South Korea very easy and also fun enough to appreciate the lovely culture. Thank you so much Kim dong-kyun, Jin eun-ji, Shin hyun-jin, Jang eun-ah, Kim so-young, Sul min-bi, Yoon seo-yeon, Yoo ju-hee, Lee sung-jin. It is however with deepest regrets that during my completion of this thesis, we heard about the sad news of Shin hyun-jin passing on. My condolences to his family.

I dedicate this thesis to my family because without them I will not be where I am right now.