MULTI-TIERED SECURITY ARCHITECTURE FOR INFORMATION INFRASTRUCTURE PROTECTION IN SELECTED COMMERCIAL BANKS IN KENYA.

BY

PAULINE KEMUNTO ROGITO

UNITED STATES INTERNATIONAL UNIVERSITY, AFRICA

SUMMER 2017
MULTI-TIERED SECURITY ARCHITECTURE FOR INFORMATION INFRASTRUCTURE PROTECTION IN SELECTED COMMERCIAL BANKS IN KENYA.

BY

PAULINE KEMUNTO ROGITO

ID 645392

A Project Submitted to the School of Science and Technology in Partial Fulfillment of the Requirement for the Degree of Master of Science in Information Systems and Technology

UNITED STATES INTERNATIONAL UNIVERSITY, AFRICA

SUMMER 2017
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University in Nairobi for academic credit.

Signed: ________________ Date: _________________________

Pauline Kemunto Rogito (ID No 645392)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: ________________ Date: _________________________

Joshua Rumo A. Ndige, PhD

Signed: ________________ Date: _________________________

Dean, School of Science and Technology
COPYRIGHT

All rights reserved. No part of this dissertation report may be photocopied, recorded or otherwise reproduced, stored in retrieval system or transmitted in any electronic or mechanical means without prior permission of USIU-A or the author.

ABSTRACT

Information technology evolution and the spread of internet connectivity have enabled globalization which allows communication and transaction of businesses across different countries. To ensure information infrastructure protection, understanding how the organizational, individual and technical aspects all together affect the outcome in information security is important. Having the necessary skill required to be able know how to react or what action to take in the event of a security incident is key. Information security incidents occur as a result of internal employee actions. In organizations, infrastructures that are considered critical are the physical infrastructure, information facilities and networks. This study endeavors to identify the weaknesses and strengths in the current information security architects being used by banks to protect information infrastructure and propose a multi-tiered security architecture to improve the protection of the information systems for the Kenyan banking sector. To realize this, an exploratory study was employed to develop a multi-layered security architecture by: Conducting a security assessment; Formulating the architecture design and Subjecting the proposed architecture to expert review to help improve the usability and effectiveness of the proposed architecture. The study findings indicate that the banking institutions security personnel do not have sufficient skills and knowledge that is important for them to be able to understand their duties and responsibilities. The institutions are working under the belief that a network firewall is sufficient for infrastructure protection. It was established form the study that there is lack of adequate security measures to protect information infrastructure. In its current design the proposed architecture incorporates the use of web application firewalls, database application firewalls, network firewalls, segmentation of networks and the dematerialized zone to restrict public access
to bank resources. With the adoption of the proposed architecture protection of the banks information infrastructure is significantly improved.
ACKNOWLEDGEMENT

I thank the almighty God for seeing me through the entire research period.

Many thanks go to my supervisor Prof. Joshua Rumo A. Ndiege for his guidance, relentless support and patience during this entire research period. I am indebted to you for your guidance and mentorship.

In addition, thanks to my family and friends for their encouragement and support during this entire period. This final document is as a result of your participation and input.
# TABLE OF CONTENTS

ABSTRACT ............................................................................................................................ v

CHAPTER 1: INTRODUCTION ............................................................................................... 13
  1.1 Background of the Problem ........................................................................................... 13
  1.2. Statement of the Problem .......................................................................................... 15
  1.3. General Objective ...................................................................................................... 16
    1.3.1 General Objective ............................................................................................... 16
    1.3.2 Specific Objectives ............................................................................................ 16
  1.4 Importance of the Study .............................................................................................. 16
  1.5 Scope of the Study ....................................................................................................... 17
  1.6 Definition of Terms .................................................................................................... 18
  1.7 Chapter Summary ....................................................................................................... 19

Chapter 2: LITERATURE REVIEW ..................................................................................... 20
  2.1 Introduction .................................................................................................................. 20
  2.2 Current Gaps in Information Security Architectures employed in Kenyan Banks .......... 21
    2.2.1 Human Factors in Information Security ............................................................... 22
    2.2.2 Importance of security awareness, training and education to ensure effective IIP .......... 23
    2.2.3 Vulnerabilities and Threat Profiles that Pose a Risk to Information Security .......... 25
  2.3 How to Develop a Multi-Tiered Security Architecture ................................................ 26
    2.3.1 Information Security Architecture Components .................................................. 28
    2.3.2 Multi-layered Security Approach in High Assurance Systems ............................. 29
    2.3.3 Protection Method for Mobile Banking for Banks and Investment Transactions .... 30
    2.3.4 Network Security ............................................................................................... 31
  2.4 Enterprise Information Security Architectures ............................................................ 33
  2.5 Research Approach ..................................................................................................... 37
  2.6 Chapter Summary ....................................................................................................... 39

CHAPTER 3: METHODOLOGY ............................................................................................. 42
  3.1 Introduction .................................................................................................................. 42
  3.2 Research Design ......................................................................................................... 42
  3.3 Population and Sampling Design ............................................................................... 43
    3.3.1 Population .......................................................................................................... 43
    3.3.2 Sampling Design ............................................................................................... 43
    3.3.2.1 Sampling Frame ......................................................................................... 43
LIST OF TABLES

Table 1.1: Weaknesses Identified from Security Architectures Reviewed............................ 39
Table 1.2: How the Literature Informs the Proposed Architecture...................................... 40
LIST OF FIGURES

Figure 1.1: Compounding Cyber Attack Progression .......................................................... 14
Figure 2.1: Security Framework by Triware Network Systems ........................................ 28
Figure 2.2: Information Security Architecture Components ............................................. 29
Figure 2.3: Security Zones for Mobile Banking ................................................................. 31
Figure 2.4: Network Security Architecture ..................................................................... 32
Figure 2.5: Gartner Enterprise Security Architecture Framework .................................... 34
Figure 2.6: SABSA Model for Security Architecture ....................................................... 35
Figure 2.7: SABSA Model for Security Architecture from a Business Driven Approach ...... 36
Figure 2.8: Steps in Designing a Security Architecture .................................................... 39
List of Abbreviations

II Information Infrastructure

IIP Information Infrastructure Protection

FFIEC Federal Financial Institutions Examination Council

COBIT Control Objectives for Information and Related Technologies

PCIDSS Payment Card Industry Security Standards

ISP Internet Service Provider

ISACA Information Systems Audit and Control Association

CERT/CC Computer Emergency Response Team Coordination Center

VPN Virtual Private Networks

DMZ Dematerialized Zone

IPS Intrusion Prevention Systems

WAF Web Application Firewall

DBF Database Firewall
**CHAPTER 1: INTRODUCTION**

Banks are highly dependent on their information systems to carry out their activities. However with this dependence has come an increase in information system attacks. Any activity that may lead to the compromise of confidentiality, integrity and availability either through loss of information, inaccuracy of the information or unauthorized access can have an adverse effect on the business.

This research looks at the following; gaps identified in ensuring information infrastructure protection; the frameworks developed by various experts to help in developing a security architecture for the protection of the organization’s information infrastructure. Information security is very important especially with the introduction of internet banking, in a banking environment because of the increase in accessibility and exposure to malicious attacks.

The main aim of this study is to develop a multi-tiered security architecture that will be used to protect against malicious attacks on a banks network, web application platform and database systems.

**1.1 Background of the Problem**

Information evolution and the spread of internet connectivity has enabled globalization which allows communication across different countries and even transaction of businesses (Johnson, Acedo, Kobourov, & Nusrat, 2015). This evolution has increased efficiency. However, with this efficiency, developing countries are now at a higher risk of cyber-attacks.

The financial system in Kenya was established in the precolonial period. Its aim was financing international trade however it grew to serve the growing population of the farming community. It all started with money lenders in the 18th century who were Indians and has now grown to be locally owned since independence (Central Bank of Kenya [CBK], 2016).
A survey by the Central Bank of Kenya in 2008 showed that there was an increase in the use of e-banking technologies; these technologies include; Automated Teller Machines (ATM’s), mobile and internet banking, electronic funds transfer, direct bill payments and credit cards. A growing partnership has also been observed between financial institutions and non-financial service providers which has enabled customers to transact through the shared bank platforms (CBK, Bank Supervision Annual Report, 2008).

The development of information technology has led to many advantages. However, despite the advantages offered; the protection of an organizations information infrastructure is not assured. Information infrastructure protection cannot be viewed only as a technical issue. Information infrastructure protection involves the configuration of systems to protect organizations information. The configuration is technical, however, the system is operated people (Parsons, McCormac, Butavicius, & Ferguson, 2010). Figure 1.1 shows a compounded cyber-attack progression from the year 1980 to 2012 by the Ministry of Information Communications and Technology in Kenya Cybersecurity Strategy (Kenya Cybersecurity Strategy, 2014).

Fig. 1.1 Compounding Cyber Attack Progression (Kenya Cybersecurity Strategy, 2014)
1.2. Statement of the Problem

Based on Kenya Cyber Security Report 2012, IT experts gave an estimation that in Kenya, there was a 95.63% increase on the number of attacks from 2010 December to 2011. This consequently led to an increase in internet security incidents (Serianu, 2012). As the saying goes, ‘a chain is only as strong as its weakest link’ (Leonard & Onyx, 2003). The Serianu (2012) report also highlights that;

Insider threats are a constant weakness in information security. The report highlights a case where employee information including their salaries was published online another case reported was a national stock exchange company’s sensitive documents were published online. This shows that local organizations have not implemented adequate methods to deal with insider threats. Most organizations still rely on traditional security devices while these devices are not able to detect and prevent web application threats (Serianu, 2012). The Serianu report 2012 lists the Government of Kenya, leading media house and four banks as victims of malicious attacks.

Organizations mainly focus on the edge protection using firewalls and work under the assumption that the firewall is able to stop all attacks (Modi, et al., 2013). However, this is not the case, the firewall is only the first line of defense that will permit or allow incoming or outgoing connections. The skills of the IT personnel are also important to ensure that they are able to understand the information infrastructure setup so as to ensure the information infrastructure is protected. Banking institutions have web applications and databases to protect. A firewall may not be fully effective in protecting against web targeted attacks or even database attacks (Khochare & Meshram, 2012). This means that not all bank web, database systems are protected.

This study focuses on providing a multi tired security architecture that will protect the web application platforms and database platforms from malicious attacks.
1.3. General Objective

1.3.1 General Objective

The general objective is to identify the weaknesses and strengths in the current information security architect being used by banks to protect information infrastructure and propose a multi-tiered security architecture to improve the protection of the information systems for the Kenyan banking sector.

1.3.2 Specific Objectives

To achieve the above objective, the following specific objectives are be pursued;

i. Asses the current gaps in information security architectures used by the banking sector in Kenya.

ii. Develop a multi-tiered security architecture to help improve information infrastructure protection in the commercial banking sector in Kenya.

iii. Evaluate the effectiveness of the developed architecture in helping to improve the Information Infrastructure Protection in the Commercial Banking Sector.

1.4 Importance of the Study

The 2012 Kenya Cyber Security Report shows the following local cyber threat trends; Kenyan ISP spamming, phishing and poor reputation scores, botnets, viruses, trojans, worms and botnets, insider threats and credit card fraud, increase in global vulnerabilities and threats, VoIP PBX fraud, social engineering, denial of service attacks, online and mobile banking attacks, database breaches, poor identity and access management.

In 2013, the threats identified in by the Serianu cyber intelligence team were; insider threats, VoIP PBX fraud, denial of service attacks, botnet attacks, online and mobile banking threats, mobile money fraud and cyber espionage (Kigen, Kisutsa, Kimani, Mwangi, & Shiyayo, 2014)
Kabeberi (2015) in one of the cyber security reports states that with the increase in connectivity to the internet, cyber security threats have consequently increased, these threats are malware attacks, social engineering scams, financial fraud and phishing. This has been made possible because organizations are interested in market share and not on measures to take for information protection (Kigen, et al., 2015).

Given that attacks are getting more sophisticated with the advance in technology and connectivity, securing the information infrastructure (II) cannot be overemphasized. This research endeavors to evaluate the gaps in the security frameworks implemented to protect II then develop a multi-tiered security architecture that can be more effective in protecting II. It is expected that as a benchmark study, the findings and developments will be integrated in the subsequent protection of banking infrastructure. The research on securing information infrastructure in Kenyan banks plays a crucial role in assisting information security officials identify the vulnerabilities in their II.

This study outlines the current challenges in information security and the loop holes that exist in the implemented security architecture compared to the set frameworks. It also provides an avenue through which information security engineers and managers are able to identify the II and evaluate whether their II is protected with the aim of improving information infrastructure protection (IIP). This is especially useful since not many studies of this nature have been undertaken in Kenyan banking institutions.

1.5 Scope of the Study

This study is limited to Kenya’s banking sector’s information infrastructure, within the last five years. It shall focus on the development of the banking sector in the past five years, the evolution of threats in the last five years and the architectures and frameworks that have been used to protect information infrastructure in that period.
The sample size is limited to four banking institutions in Kenya due to the constraint of time and willingness of banks to participate in external research. The information infrastructure and the practices or security measures that have been put in place to ensure information security across these institutions are compared. With the aim of evaluating whether their security structures are protecting the II.

The actual bank names are not used due to legal constraints to ensure privacy and confidentiality is maintained. As a result pseudo names are used.

1.6 Definition of Terms

**Information infrastructure (II)** – This is the communication network, associated software and information resources that are used in an organization to enable communication or interaction between business or organizations and people.

**Information infrastructure Protection (IIP)** – This is the method of ensuring that the communication network, associated software and information resources that are used in an organization to enable communication or interaction between business or organizations and people are not vulnerable to attacks.

**Vulnerability** – This is any weakness in a system that makes it possible for a threat to cause it harm.

**Threats** – This is any event that tries to exploit any know vulnerabilities.

**Attack** – This is an event on a system whose main aim is to destroy, steal or alter information on a system.

**Multi-layered security architecture** – A setup that uses different security technologies and measures to protect against different vectors of attacks.
1.7 Chapter Summary

Attacks on information systems are on the raise. In developing countries information security has not been a primary focus. With the introduction of internet and mobile banking, information security is now a necessity because banks are becoming targets for attacks. However, even with the knowledge that information security is important, banks are yet to employ the proper measures to ensure there is protection of information. Confidentiality, integrity, availability and accountability are very important in ensuring information security is achieved. It is important that security personnel have the required skills to be able to effectively ensure that information infrastructure protection is achieved because understanding how the organizational, individual and technical aspects all together affect the outcome in information security is important.

The following chapter shall look at the challenges around information security, the strengths and weaknesses in the current architectures that are used in banks so as to be able to develop an architecture that helps to protect information infrastructure more effectively and reduce the risks that banks are currently being exposed to.
CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

A research carried out on the consequences of IT control weakness on management of information systems focusing on Sarbanes – Oxley Internal controls showed that, the weaker the IT controls, the lower the information quality produced. Hu, Dinev, Hart, and Cooke (2012) also states that understanding how the organizational, individual and technical aspects all together affect the outcome in information security. According to Hu et al. (2012), more information security incidents occur as a result of internal employee actions through insider attacks or lack of security awareness.

In organizations, the physical infrastructure, information facilities and networks are considered critical infrastructures. Developing countries are now facing increased cyber-attacks, therefore protecting the information infrastructure and the network is very important. Information infrastructure attacks include activities like unauthorized access to systems or information, destruction, modification or sharing of confidential information and also denial of service (Lopez, Setola, & Wolthusen, 2012).

Studies by a trade association for United Kingdom banking sector (Home, 2014) indicated that banks are increasingly becoming the primary focus of attacks and with the increase in internet connectivity. Banks have to ensure that their information infrastructure is protected against targeted attacks. However, even as information security personnel in developing countries there are challenges. Based on a survey by Khan and Barua, (2009) carried out in Bangladesh major challenges identified were:

- Lack of adequate knowledge
- Lack of training
- Lack of preparedness for an attack
- Under-prioritization of information security
- Lack of resources to carry out system updates

There are various information security governance frameworks widely adopted in the banking industry these are FFIEC, COBIT, ISO27002 and PCIDSS, (Ula, Ismail, & Sidek, 2011). These frameworks have been developed to guide information security personnel on how to best protect information infrastructure especially in banks. The question is, has the banking sector in Kenya taken into consideration the best practices as provided by the architectures? It is however important to note that the architectures developed are based on frameworks that are used to ensure there is Information Infrastructure Protection (IIP).

People in the organization lack the necessary security practice knowledge this poses a great information security threat (Veiga & Eloff, 2011). This study aims to develop an architecture that takes into consideration the information security frameworks developed for banking industries to help improve the protection of information infrastructure.

2.2 Current Gaps in Information Security Architectures employed in Kenyan Banks

A study carried out in Bangladesh (Khan & Barua, 2009) listed the following as challenges in ensuring information security is achieved; Lack of adequate knowledge, lack of proper training, failure to regularly upgrade the solutions in place and lack of security professionals.

It is important to ensure that an organization promotes positive security behavior. There is a need to understand the usability issues experienced users, this is an effective way to ensuring that information security personnel are well trained and equipped to effectively facilitate information infrastructure protection. Security awareness is a good way to promote IIP, this helps prevent attacks.
This study identifies the issues that are faced in information infrastructure protection. This issues range from users, skills, security awareness and threats that information infrastructure are exposed to.

### 2.2.1 Human Factors in Information Security

Human beings have been said to be the weakest link in information security. Information infrastructure protection focuses on the protection of confidentiality, integrity and availability. Despite the number of security controls put in place, organizations still experience security breaches (Kruger & Kearney, 2006). This is greatly dependent on system users’ actions, these users contribute greatly to insider threats as highlighted in the Serianu reports over the years. The users focused on in this study are security administrators. This is because they are the people involved with ensuring the security policies are enforced (Schneier, 2000). This section shall look at the human factors that are brought about by lack of information security skills that can lead to security breaches in systems. Users are especially vulnerable to social engineering (Huang, Rau, & Salvendy, 2007).

In a literature review on User Security Behaviors, Stanton, Stam, Mastrangelo and Jolton, (2005), affirm that many information security experts believe that enforcing good user behavior makes information security effective within an organization. Stanton, et al, (2005) have described security behavior using a two-factor taxonomy. These two factors are: intentionality and technical expertise. Intentionality examines whether the actions of the user are malicious or beneficial, while the technical expertise focuses on the knowledge and skills of the user. The skills acquired can be of a positive effect ensuring IIP or a negative effect leading to IIP compromise.
2.2.2 Importance of security awareness, training and education to ensure effective IIP

In order to secure information systems and networks, an organization has to employ a team of information security persons. With the development of technology and continuous evolution of threats to an organization, it is very important that information security experts constantly improve their skills in order to anticipate and deal with various information security threats. Khan and Barua, (2009) demonstrate that efforts to protect systems are not effective due to lack of skill. Raising security awareness, giving the necessary training and education is very important in ensuring that IIP is effective to help reduce the human factor threats. A report by the National Institute of Standards and Technology (2002) states that learning to gain skills starts form awareness, then training, evolving to education from where it is used for personal development. The information security officer should be able to;

1. Develop policies that protect the business from risks.
2. Educate user of their responsibilities towards effective IIP.
3. Have the skills to monitor and manage the information security.

Security awareness is focused on information security personnel so as to enforce good security practices. Training as defined by NIST (2002) is a process that strives to produce relevant and needed security skills. Training seeks to teach skills that allow an individual to carry out certain functions. On the other hand, awareness aims at getting an individual to focus on an issue. Bensnard and Arief (2004) emphasize that education of staff is important because it makes people aware of the effects of their actions thus ensuring that people are conscious of the threats and probable damages.

In a 2014 report by Information Systems Audit and Control Association (ISACA) titled “The Growing Cyber security Skills Crisis,” shows that despite the increase in threats that organizations
are facing, many organizations do not seem to be concerned about increasing the skills of their cyber security staff. According the report the reasons for lack of skill in the information protection field are that:

- There are too many jobs but few qualified professionals.
- Few institutions exist that can produce individuals with the necessary skills to enforce information security.
- There is very little technological know-how on the implementation and management of information security systems.

As a result, there was a 62% increase in the number of breaches between 2012 and 2013.

A 2013 Global Information Security Workforce Study carried out by International Info System Security Certification Consortium (ISC)² shows that people are an important aspect in information security. According to the report, to secure the information infrastructure, it is important to:

- Have management support the security policies.
- Have qualified security staff
- Adhere to the security policies.
- Train staff on security policy.
- Have secure software development.
- Have finance and insurance to cover the institution against losses.

To have a balance between information security and skills the following challenges have been identified that need to be addressed to ensure there is effective information infrastructure protection (Piggin, 2015):

- Raising awareness of the risk
• Designing the security
• Culture
• Usability
• Understanding the opportunities and risks of the internet of things.

2.2.3 Vulnerabilities and Threat Profiles that Pose a Risk to Information Security.

Information infrastructure protection is aimed at protecting the information infrastructure of an organization from threats and also ensure that systems are not vulnerable to attacks. Michael and Herbert, (2011), defines a threat as any entity that presents a danger to an asset. Liu and Cheng, (2009), define a vulnerability as a weakness that can be exploited to gain access to information. For a vulnerability to exist, it means there is a gap in the system security. Threat sources, attackers, their intentions and effects have changed with the advance in information technology (Yeh & Chang, 2007). Changes in technology have significantly led to the increase of vulnerabilities. A previous research by US Computer Emergency Response Team Coordination Center (CERT/CC) has noted that security vulnerabilities have increased exponentially from 171 to 7,236 between 1995 and 2007.

With an increase in technological advancement, there are four main effects of threats in an information infrastructure (Yeh & Chang, 2007); interception, interruption, modification and fabrication. Other effects can also be disclosure and destruction. Threats can further be classified into three categories, natural threats, human caused and technical. Natural threats are threats that are posed by natural conditions like climate changes, geographical hazards amongst others. These can cause physical damage to the information infrastructure.

Human threats are threats that are considered as malicious acts, this can include acts of terrorism, explosions and product tampering. Information security does not only involve protection of
infrastructure but also includes people. In relation to the role of the individuals in a security process, the individuals as potential targets or the individuals as attackers either knowingly or unknowingly (Solms & Niekerk, 2013). Lastly, technical threats involves incidents like system failures (Snedaker, 2007).

A successful exploitation by a threat can have direct or indirect effects to information infrastructure. Direct effects would cause the disruption of infrastructure functions while indirect effects are caused by attacks on other infrastructure because of their interdependencies (Robles, Choi, & Cho, 2011).

2.3 How to Develop a Multi-Tiered Security Architecture

According to Thorn, Christen, Gruber, Portman, and Ruf, (2008) a security architecture is a design that is structured in a manner that integrates various components in an organization for its benefit. The architecture should be: financially sensible (based on return on investment), manage risks, implement best practices and follow legal requirements.

Farah, (2005) outlines five steps that are involved in designing a security architecture. The first step is analyzing the current security architecture. This step enables an organization to identify the threats and vulnerabilities that their systems are exposed to and also verify if the current control measures are effective. The second step is formulation of the security architecture design. The design developed in this step entirely depends on the finding of the first phase. There are two types of security architecture designs involved. The first is the logical architecture; which involves the processes, technology and people involved. Understanding the flow of information is also important in developing the logical architecture. The second security architecture design is the physical design which involves coming up with a diagram that illustrates the various firewalls, networks components and connections that are related in the architecture. The third step in
designing a security architecture is coming up with policies and procedures which are meant to define what is to be protected based on the organization’s needs. Fourth step is implementation of the architecture design. The fifth step after implementation is integration of the security practices so as to deliver security.

The important part however is know the basic requirements of a security architecture. Angelo, (2001) States that a security system should ensure or enforce confidentiality, integrity availability and accountability.

For us to be able to develop an architecture that will help with information infrastructure protection in banks, there is need to know the guidelines or regulations that have been put in place. These regulations are referred to as frameworks. An IT security framework is a chain of processes used to outline the policies and procedures for protecting the information infrastructure. A security framework is a guide for securing information (Granneman, 2013).

According to Benson Yeung (2012) in an article ‘The Security Framework for Information Technology’, there are two major causes of vulnerabilities in information security. The first is mistakes by users and IT engineers who most of the time are not trained. The second is the lack of proper guidelines for information technology professionals on how to properly implement information infrastructure protection.

IT professionals may not understand the security issues they face in their organizations and how to resolve these issues, the complexity of information technology has made it more difficult (Yeung, 2012). Figure 2.1 shows a general security framework developed by Triware Networld Systems
Information Security Architecture Components consists of the organizations infrastructure, policies, standards and procedures, security baselines, user awareness and training and compliance. These components must be considered when developing architecture. This enables information security personnel to identify the specific components they are developing the architecture for (Killmeyer, 2006).
For information security to be effective one must have a holistic approach that fits the company’s profile (Eloff & Eloff, Information security architecture, 2005). First, identification of the critical systems for operations in the organization can be done by knowing the important roles and responsibilities of the key personnel in the organization. Secondly policies, standards and procedures are an important aspect of creating an architecture design because they define the controls that are supposed to be enforced in the organization.

It is important for the organizations to know why the architecture is necessary and what it is protecting it from. It is important to identify the risks that organizations can be exposed to and also enable them to know the strengths and weaknesses in the information infrastructure. This risk analysis needs to be done for processing platforms, databases, networks and applications. Figure 2.2 is a diagrammatical representation of the information security architecture components mentioned.

![Information Security Architecture Components](image)

**Fig 2.2 Information Security Architecture Components (Killmeyer, 2006)**

### 2.3.2 Multi-layered Security Approach in High Assurance Systems.

Previous attempts to develop high assurance computer systems have been based on the security kernel which is responsible for overseeing the entire systems’ security. However, this approach
was not feasible because it led to a system that was not flexible and had a complex operating system, this made the system difficult to evaluate. A multi-layered security framework is able to support many levels of security by creating separated layers, with each layer enforcing its security policy (Alves-Foss, Taylor, & Oman, 2004).

The layered architecture has the kernel, secure middleware and an application layer. The setup is based on separate processing units. The partitioning kernel layer is responsible for separating processes on a processor to multiple processing engines, making each partition seem like it has its own processor (Alves-Foss, Taylor, & Oman, 2004). The partitions are separated using time. The middleware layer handles all communication infrastructures between clients and objects, location and identification of objects, delivery of data and connection management. Finally the application layer consists of applications that are used to implement security policies. These applications are supported by the kernel and the middleware (Alves-Foss, Taylor, & Oman, 2004). However the application layer is independent and enforces security without affecting any layer (Boeing and Collins, 2003).

2.3.3 Protection Method for Mobile Banking for Banks and Investment Transactions

A mobile banking system consists of a mobile banking unit and a center for processing the banking transactions and storing data. This functionality includes ATMS, online banking and mobile transactions (Jin & Xianling, 2008) as shown in figure 2.4.

According to Jin and Xianling, (2008), mobile banking has two security zones. The first is the mobile security zone which involves the people who use the mobile banking platform to carry out transactions. The second is the banking security zone which lies on the banks end. In this zone, transactions are carried out between the banking system and the user.
In mobile banking protection against various threats is important. These threats are:

- Information leakage, loss or distort
- Incomplete information caused by unstable mobile transmission channels
- Denial of service attacks

Information security needs of a mobile banking system are evidently different from the information security needs of the banks’ network. Network protection strategy cannot be used for mobile banking (Jin & Xianling, 2008). There is a need for new technology and safety measures for mobile banking. Mobile banking needs encryption technology to ensure there is data privacy, system and data integrity assurance in cases where an attacker may try to gain access to alter information. Authentication is also important so as to ensure that transactions are carried out by authorized individuals only. Digital signatures are important so as to ensure there is data authentication and non-repudiation. Finally, a wireless public key infrastructure which uses a set of standards for key and certificate management, is needed to establish secure communication to the banking system (Jin & Xianling, 2008).

### 2.3.4 Network Security

Network security architectures have been developed for protection against hackers, malicious code and other attacks that may cause failure or lack of confidentiality, integrity and availability (Stawowski, 2009). The network architecture described in this section is a multi-tiered network.
security architecture that consists of a web, application and database server zones. The web server is used by customers who wish to carry out transactions, application servers are used for data processing of customers or client requests and the database server is essential for data storage.

Routers, firewalls, data encryption using Virtual Private Networks (VPN), Intrusion Prevention and load balancing for server acceleration provide network services that are needed in an organization. This is the first group of information infrastructure that needs to be protected. The second group is the core network services or internal network service which includes servers and application and databases together with the intranet.

Fig 2.4 Network Security Architecture (Stawowski, 2009)
2.4 Enterprise Information Security Architectures

In a document published by Gartner on Information Security Architecture (2011) states that for an enterprise information security architecture to be effective it should be based on the enterprise architecture principle. This is an important factor in improving information security planning, implementation and operations. Enterprise architecture principle helps in making security design decisions aligned with business requirements. The main focus is on maintaining and developing evolving requirements, models, templates and principles because security architecture is a continuous process.

Enterprise Information Security Architecture (EISA) frameworks can be examined from an abstraction level meaning from a general idea point of view. An abstraction level examination includes holistic methods versus partial methods.

Partial methods can be divided into four categories;

- Security policies and configuration management these concern risks, directions and procedures and also defines penalties and countermeasures in the event of a transgression (Rees, Subhajyoti, & Spafford, 2003).
- Security of enterprise services which focuses on securing enterprise information because the automation of service leads to exposure of enterprise information. It is important to secure web services and there are solutions specific to handling the same (Nakamur, Hada, & Neyama, 2002).
- Security role management and access control.
- Security assessment and requirements engineering which servers the purpose of assessing the current situation of enterprise security, evaluating information assets and also risk assessment (Shariati, Bahmani, & Shams, 2010).
Holistic methods include the following frameworks Gartner, Sherwood Applied Business Security Architecture (SABSA) which is a proven methodology that is used for developing a security architecture focused on risk and opportunity that is business driven (SABSA Institute, 2017). Third is RISE which is a threat based and risk managing method.

There are three levels of abstraction defined by Kreizman, (2011) namely conceptual logical and implementation which enable planning and designing of a security architecture framework. These three levels can be used in three different views; business, information and technical. Gartner insists on compatibility between the levels and views. Figure 2.5 shows a general description of the structure and framework of an enterprise information security architecture by Gartner illustrating the collaboration between the three level and the three viewpoints.

![Gartner Enterprise Security Architecture Framework](image)

*Fig 2.5 Gartner Enterprise Security Architecture Framework (Kreizman, 2011)*

SABSA layered architecture has six layers. These layers are; contextual, conceptual, logical, physical, component and security service management which cuts across. The SABSA
methodology is based on a business attribute profile which consists of the business requirements and the required guidelines.

The contextual layer looks at the development of the architecture from a business view. Its aim is to ensure that the goals, assets and objectives are enhanced and secured. The conceptual layer takes an architectural view, looking at the risks, risk management, process assurance, roles and responsibilities, domain and time management. The logical layer focuses on the processes required to achieve security these include identifying information assets, risk management policies, processes and services. The physical layer consider the data assets, risk management practices, human interface and ICT infrastructure. Component layer incorporates the ICT components, tools and standards for risk management, processes and personnel management. Finally the security service management aims to ensure that all layers are secure (Sherwood, Clark, & Lynas, 2015).

Figure 2.6 is a pictorial representation of the SABSA model for security architecture.

Fig 2.6 SABSA Model for Security Architecture (Sherwood, Clark, & Lynas, Enterprise Security Architecture Whitepaper, 2009)
Figure 2.7 is a representation of the SABSA model from a business driven approach.

**Fig 2.7 SABSA Model for Security Architecture from a Business driven Approach** (Sherwood, Clark, & Lynas, Enterprise Security Architecture A Business-Driven Approach, 2015)

The RISE methodology was developed for information security management across the enterprise. This has been made possible by incorporating both security and privacy in the business process, however this method does not focus on technical details (Shariati, Bahmani, & Shams, 2010).

Today with the evolution of technology, IT is included in all parts and activities of an organization therefore any IT management system must enable an organization to achieve its goals and missions with the knowledge that business environments and information systems are changing and growing.

Khayami, (2011), recommends the following properties be included in an enterprise architecture:

**Alignment:** Information communication technology is used to ease the management activities in an organization. Therefore it is important to have the technology used aligned with the business.
**Convergence:** Information technology in an organization must all serve the purpose of achieving the organization's goals and missions.

**Maintainability:** the technology used should be flexible to accommodate the changing needs of a business.

**Integrity:** Data integrity and application integrity are very important.

**Reliability:** Availability of services is important in any organization, therefore accessibility to services must be included.

**Efficiency:** helps to ensure resources and time are well maintained.

**Security:** Focuses on protecting information and application systems from unauthorized access, use, modification, disruption modification and destruction.

**Usability and Implementability:** this must be considered so as to factor in the necessary time and expense needed for deployment.

### 2.5 Research Approach

In order to come up with a security architecture that aids with information infrastructure protection, one must look at the various factors that influence IIP. Therefore one must understand the issues and challenges that are there in the current IIP so as to be able to identify the problem that is to be focused on. Just identifying the issues and challenges is not enough; one has to look at the security frameworks that are meant to be used for banking institutions so as to ensure that the security architecture developed is in conformity with the set guidelines. After identifying the challenges and the frameworks, it is also important to identify the gaps that are present in the current architecture because identifying the gap is important in the development of an architecture that
will serve the purpose of filling in the current gaps. This process will facilitate the development of a suitable security architecture for banks.

Various steps have been outlined by Farah (2005) that can be used in designing a security architecture:

1. Analyzing the current security architecture.
2. Formulation of the security architecture design.
3. Coming up with policies and procedures.
4. Implementation of the architecture design.
5. Integration of the security practices.

These steps shall be adapted in the development of an architecture that can be used to help information improve infrastructure protection. The steps are as follows:

1. Conduct a security assessment.
2. Formulate a security architecture design.
3. Evaluate the effectiveness of the proposed architecture through expert feedback.
Fig 2.8 Steps Adapted in Designing a Security Architecture from Farah, (2005)

2.6 Chapter Summary

There are various guidelines that have been set for protection of web applications, networks and databases separately. The major challenge being faced by the banking sector is that guidelines have been set, but they cannot be used to deliver information security if the security personnel themselves do not have the skills required to implement.

To ensure that an organization promotes positive security behavior it is important that information security personnel are well equipped to effectively facilitate IIP. Appropriate training needs to be offered to improve the skills of the security personnel. Challenges identified by Piggin (2015) that need to be addressed so as to ensure effective information infrastructure protection are:

- Raising awareness of the risk
- Designing the security
- Culture
- Usability
- Understanding the opportunities and risks of the internet of things.
Threats are always evolving because attackers are always designing new ways to exploit vulnerabilities on systems. It is important to understand the threats, the entities in information infrastructure protection against threats.

Table 1.1 gives a view of the gaps identified from the architectures reviewed in this chapter.

Table 1.1 Gaps/Weaknesses Identified from Security Architectures Reviewed.

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Description</th>
<th>Gap/Weakness</th>
<th>Illustrative Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Architecture</td>
<td>The components of information security architecture are the infrastructure, policies, user awareness and training, compliance and security assessment.</td>
<td>Very little knowhow as there is no common standard architecture that exists.</td>
<td>(Eloff &amp; Eloff, Computer Fraud &amp; Security, Information Security Architecture, 2016)</td>
</tr>
<tr>
<td>Multilayered Security Infrastructure for IoT</td>
<td>Every layer i.e. application layer, network layer and the terminal must have encryption, decryption and access control mechanisms.</td>
<td>Method of encryption used does it secure the systems put in place how is the decryption and encryption process is it ensuring efficiency?</td>
<td>(Baharon, Shi, &amp; Jones, 2015)</td>
</tr>
<tr>
<td>Network Security Architecture</td>
<td>There are 3 sections that require protection, the perimeter which includes routers, dematerialized zone and internal which contains database and application servers. Security mechanisms that can be used are firewall, network and web application firewalls and intrusion prevention systems.</td>
<td>There is no standard architecture.</td>
<td>(Stawowski, 2009)</td>
</tr>
</tbody>
</table>
Table 1.2 below gives brief illustration of how the literature informs the proposed architecture.

*Table 1.2 How the Literature Informs the Proposed Architecture.*

<table>
<thead>
<tr>
<th>Literature Item</th>
<th>How it Informs the Proposed Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current issues</td>
<td>Gives an understanding of what has hinders the effective protection of information infrastructure leaving it vulnerable to attacks.</td>
</tr>
<tr>
<td>Information security trends</td>
<td>Informs on how threats to information infrastructure have evolved over the years, now making information infrastructure protection important to every organization.</td>
</tr>
<tr>
<td>Security architectures</td>
<td>Gives an overview of what architectures have been developed over time to help guide in information infrastructure protection with the aim of developing and architecture that is aimed at improving IIP.</td>
</tr>
</tbody>
</table>

The next chapter shall discuss the methodology used to carry out the study including the sample size, data collection and research process.
CHAPTER 3: METHODOLOGY

3.1 Introduction

This section seeks to outline the methods used by the researcher to carry out the study and achieve the specific objectives as outlined in chapter one. It includes the research design, study setting, research strategies, and research population.

3.2 Research Design

The study is exploratory in nature because there are various security architecture that have been developed however these architectures give a general approach. This study was focused on the technical approach developing an architectural design that can be implemented in banks. It is descriptive because it shall explain the various challenges and issues facing IIP implementation in the Kenyan banks. It looks at the threats that their information infrastructure is exposed to with the aim of coming up with an architecture that is best suited to protect critical information infrastructure.

The study was exploratory when it comes to developing a multi-layered security architecture for protecting the information infrastructure. To be able to come up with an architecture that will help improve the protection of information infrastructure, execution will be done in various phases:

1. Conducting a security assessment
2. Formulating the architecture design which is based on the findings of step 1.
3. To test whether the design is effective by getting expert feedback.
3.3 Population and Sampling Design

3.3.1 Population
The target population that was engaged during the security architecture development phases was the information infrastructure and information system security teams of banks who are responsible for maintain infrastructure like network, databases and web applications.

This population is involved in the research process to help understand the current protection methods used and determine whether the same is effective. Information security experts are also be involved in the process of evaluating whether the architecture is effective in protection of critical infrastructure.

There is a total of 41 Commercial Banks Licensed by the Central Bank of Kenya. This study involves four commercial banks with each bank having at least five IT personnel.

3.3.2 Sampling Design

3.3.2.1 Sampling Frame
The sampling frame was a list of all persons involved with the network, database and web application functions in the selected Kenya Commercial banks.

3.3.2.2 Sampling Technique
My sampling technique used was purposive, which is a non-probability sampling method. This involves selecting the people to be used to carry out the study. Consequently the sample was carefully chosen to include personnel with the following qualifications: network administrator, database administrator and web application administrator

3.4 Data Collection Methods
To carry out the study, secondary together with primary data was collected. The security reports generated by Serianu on cyber security together with reports generated by different institution
pertaining to information security will be the source of the secondary data. This provides a record of past and current efforts in IIP. These reports highlight the current security issues in order to understand the treats so that they can be effectively stopped. The secondary data is used to determine whether the architecture developed is able to protect against the current threats. Primary data was obtained through interviews that were be carried out with information security personnel of the banks involved in this study.

### 3.5 Research Procedures

To have an understanding of the information infrastructure in the banks, an interview with IT personnel was carried out. Interviews were be carried out based on availability of personnel in the four banks. The study adapts a few steps for developing an information security architecture developed by Farah (2005). Appendix I contains the interview questions asked to enable understanding of the current bank architecture.

![Security Assessment Diagram]

**Security Assessment**
- Study the current information security architecture.

**Architecture Design**
- Develop a security architecture that offers information infrastructure protection.

**Security Assessment of the Architecture Design**
- Evaluate the proposed architecture through expert feedback.

### 3.6 Data Analysis

The data analysis method used in this study was a thematic analysis. This involves highlighting or examining the patterns within the data collected from the four banks.
3.7 Chapter Summary

This study shall be descriptive and exploratory. The target population is the information infrastructure team of banks who are responsible for maintain infrastructure like network, databases and web applications.

The sample size was four banks. Data collection involved use of secondary data through the security reports generated by Serianu on cyber security. These information will therefore be used to determine whether the architecture developed at the end is able to protect against the current threats. Development of this architecture involves adapting some steps for developing an information security architecture as outline by (Farah, 2005)
CHAPTER 4: MODEL

4.1 Introduction

This chapter covers the information collected from the interviews carried out on the current II of the four banking institutions. The information collected relates to the research questions which the study was guided by.

To help in ensuring that II is protected effectively against attacks that can be targeted to banking institutions, an architecture was developed. Information was gathered through interviews carried out with the information security personnel in each bank. The information collected were aimed at identifying the issues that the current information security personnel are faced with together with the observed global trends so as to be able to come up with an architecture that can be used to improve IIP.

The first section looks at the information infrastructure that is found in banks this is the infrastructure that needs to be protected. The second section will focus on the architecture that can aid in IIP.

4.2 Analysis

This section seeks to document the banking environment that enables the banking institutions to carry out the various functions as per the information collected from the interviews carried out. The first step was to gather the information that was needed for the assessment of the current architecture. Interviews were done with a security personnel in each bank.

This sections focus is phase 1 and 2 as described in security architecture in the preceding topic, the current architecture in four banks shall be evaluated, to ensure whether the security architecture design is effective. The environment that will be described in this section was arrived at by analyzing the current infrastructure of banks and understanding their functions.
4.2.1 Current Bank Architectures
This section gives a diagrammatic representation of information infrastructure in the banks that were involved in the survey. These banks have branches in all major towns across the country. The architectural designs generally show all the systems that enable operations in the banks and how they are subsequently protected. This will help in understanding the security gaps in the current banking architectures and also appreciating the need for an architecture that will give better protection.
4.2.1.1 Bank A Architecture Design

Bank A has its head office located in Nairobi Central Business District with a total of six branches in the following cities Nairobi, Diani, Malindi, Nyeri, Meru and Eldoret. This bank has a total of 9 Information Technology personnel in the head office.
4.2.1.2 Bank B Architecture Design

Bank B has its head office located in Nairobi Central Business District with a total of seventeen branches in various towns Nairobi, Kiambu, Machakos, Kajiado, Diani, Malindi, Nyeri, Meru, Kisii and Eldoret. This bank has a total of 15 Information Technology personnel in the head office.
4.2.1.3 Bank C Architecture Design

Bank C has its head office located in Nairobi with 56 branches across the country located in and not limited to Nairobi, Nakuru, Mombasa, Kisii, Kisumu, Eldoret, Kajiado and Machakos.
4.2.1.4 Bank D Architecture Design

Bank D has its head office located in Nairobi Central Business District with a total of eighteen branches in various towns Nairobi, Mombasa, Kisumu and Nakuru. This bank has a total of 5 Information Technology personnel in the head office.
4.2.2 Assessment Details

Internet Service Providers (ISP) are companies that provide internet connections to an organization. Most organizations have a single ISP.

Checkpoint next generation firewall is a network security solution that is able to:

- Restrict or allow user based on rules defined.
- Identify users when linked with an organization’s LDAP server.
- Control applications accessed by users so as to stop threats that users are exposed to while on the internet and
- Allow for VPN connectivity.

Secondly, it has data loss prevention capabilities that classify information in an organization and preventing loss of sensitive information from the organization. Third, it has the capability to stop threats using Intrusion Prevention System (IPS), Uniform Resource Locator (URL) filtering, application control, antivirus, antibot and email security. Lastly, the firewall has threat emulation and extraction capabilities to protect against zero day attacks (Checkpoint, Checkpoint 4600-Appliance Datasheet, 2017).

Authentication is done using username and password. The checkpoint firewall has three ports: one for external connections, the other port dedicated to the dematerialized zone (DMZ) network and another port for internal LAN (Local Area Network) connection. The firewall is able to do load balancing and failover on the external connection to ensure business continuity in the event of an internet outage.

The internet banking checkpoint firewall has one port for the external connection and has another internal connection for the bank’s web server and another connection for the Cisco ASA firewall.
The DMZ helps protect the inside network from possible attacks, devices placed in the DMZ are those that are accessible to the public. Using a DMZ ensures that public access to resources in this zone are restricted to the zone as compared to having the resources at the internal section.

Cisco ASA offers next generation firewall services including application visibility, web security, botnet filter and intrusion prevention, these are best for network security. Next generation firewall services are capable of providing visibility and a detailed access control that is needed to secure the devices and applications on the network. The web security feature is able to restrict access to web applications based on the reputation of a site. It also has Intrusion Prevention System (Cisco, 2016).

Cisco ASA 5525x in bank C is used for VPN connection, while the ASA 5545x is used for inspection of traffic coming into and leaving the network, application filtering and IPS is also enabled. The ASA firewalls are set up in high availability to ensure that there is no termination of services when one device fails this helps ensure there is availability.

Fortigate Next Generation Firewall uses Fortiguard security subscription services which enables the device gain visibility and web and uniform resource locator control and also protect against malware attacks. This can be done using the following features; user-identity awareness, intrusion prevention, antivirus, web filtering and advanced threat detection (Fortinet, 2017).

The Forti-Manager is used to generate reports for top level management purposes. This enables one to have a summary of incidents, user activity and network activity from the fortigate firewalls.

For Bank C, the device is configured as the second security tier for edge network protection, it is placed after the ASA firewall. It is configured with access rules for network access, sites to be blocked or allowed are configured according to the organizations policies.
Switches have Virtual Local Area Networks (VLANs) configured with each IP subnet in its own VLAN. The use of VLANs allows for network segmentation enabled the administrator to identify what devices use a specific subnet making management of the network easy. Some switches are also used for layer two extension especially to connect more than one server.

Results Bank A

The operation system is hardened and is up to date. Only ports used in internet communication are open. Web applications are blocked according to the banks internet usage policy, IPS software blade is enabled to protect against intrusion. Antibot and email security features are not enabled due to high CPU usage when these features are enabled causing performance issues.

The CISCO software is up to date however the only feature enabled or in use is the next generation firewall that contains rules for access control. This system is underutilized and is not appropriate to use for securing the database application and web server. This firewall is good for network edge security and has no database, application or web server protection capabilities.

Recommendation Bank A

The checkpoint firewall needs to be upgraded to one with better processing capability. This can also enable activation of other features that can help in securing the network. The firewall is specifically designed for network security and has poor controls to secure the organizations systems against web server, database and application server attacks. The organization should look into the acquisition of a database and web server firewall.

A database firewall and web application firewall is necessary to secure the complete information infrastructure of the bank.
**Result Bank B**

The operation system is hardened and is up to date. Most policies have all ports open for communication, applications and urls are blocked according to the banks internet usage policy, IPS software blade is enabled to protect against intrusion. Antibot and email security features are not enabled due to high CPU usage when these features are enabled causing performance issues.

**Recommendation Bank B**

The current firewall hardware needs to be upgraded to one with better processing capability. So as to enable activation of other features that can help in securing the network. The firewall has no capability to secure the organizations systems against web server and database server attacks. The organization should look into the acquisition of a database and web application server firewall.

**Result Bank C**

The CISCO firewall software is up to date, the firewall is well utilized and is positioned appropriately for effective edge protection.

The setup enables Fortigate to carry out a second inspection on the internet traffic to ensure only allowed connections are getting through and to also scan for malicious activity during access. The device is good for network edge security however when it comes to web application protection and database protection this firewall is not able to protect against various web application attacks like cross site scripting, SQL injection cookie poisoning but to mention a few.

**Recommendation Bank C**

The firewall should constantly be updated to ensure all signatures are up to date so as to ensure effective protection. The organization should look into the acquisition of a database and web
application server firewalls so as to effectively secure the information infrastructure of the bank from various attacks.

**Result Bank D**

The operation system is hardened and is up to date. Most policies have all ports open for communication, applications and urls are blocked according to the banks internet usage policy, IPS software blade is enabled to protect against intrusion. Antibot and email security features are not enabled due to high CPU usage when these features are enabled causing performance issues.

**Recommendation Bank D**

The current firewall hardware needs to be upgraded to one with better processing capability. So as to enable activation of other features that can help in securing the network. The firewall has no capability to secure the organizations systems against web server and database server attacks. The organization should look into the acquisition of a database and web application server firewall.

**4.3 Modeling and Design**

The system architecture was developed based on the general knowledge collected form the interviews on the flow of information through the organization this includes the ISP connections, branch connections, routers, switches, edge firewalls, database, web application servers and other LAN connections This design will seek to ensure that all information infrastructure is protected in an effective manner.
All ISP connections are terminated on a router where routing configuration for ingoing and outgoing communication can be done. Connections form the router are then terminated to an edge
firewall. This firewall can be used to configure internet access rules including access lists for incoming and outgoing connections.

The Interfirewall switch is used to carry connections form the internet firewall, branches and also the second tier of network firewall. The second tier of network firewall is used to secure traffic coming from the branches and the internal LAN destined to servers or the internet back to the branches.

The second tier of firewall for best practice. It is a different technology from the first this will help in preventing attacks. In the event the first firewall is not able to detect an attack or violation, the second firewall should be able to. However to ensure that this is achievable it is important to note that both firewalls must always be updated with patches, bug fixes or new firewall operating systems released by the vendor.

The DMZ switch is used to host web servers which are accessed by customers over the internet. This helps ensure that the customers have no access to the banks private network reducing risks of intrusion because web server accesses does not go beyond the second tier firewall.

The Web Application Firewall (WAF) is used to protect the web server form web application targeted attacks. These type of attacks are not prevented by network intrusion detection system cards attached to the network firewall. All traffic targeted to the web server has to go through the WAF. This ensures that the traffic is inspected the permitted to go to the web server.

The Database firewall (DBF) is used to protect the databases that are used to run the bank for example, databases that contain customer information. The DBF is able to protect against database targeted attacks, process queries to the database from the web application and allow fetching of information provided the connection is allowed by the DBF. All connections to the databases have to go through the DBF to be inspected.
The manager is a device that can be used to manage the WAF and DBF in terms of rule or policy management. Configurations for the WAF and DBF can be done through the Manager provided they are mounted to the Manager. This makes management of the devices easier as compared to having to log into each device for management.

The core switches are used to enable communication to and from the users, servers and the internet through the respective firewalls. This enables communication from the inside networks to external networks and also for segmentation of networks within the organization.

**4.4 Proof of Concept**

This section will focus on validation of the architecture designed. To find out whether the developed architecture is able to facilitate and achieve information infrastructure protection, an interview was carried out with security experts in different organizations.

Below is a profile of the experts involved.

<table>
<thead>
<tr>
<th>EXPERT ID</th>
<th>YEARS of EXPERIENCE</th>
<th>PROFESSIONAL QUALIFICATION</th>
</tr>
</thead>
</table>
| Expert 01 | 8 years              | Certified Information System Auditor (CISA)  
Certified Information Security Manager (CISM)  
Certified Ethical Hacking (CEH)  
Certified Information Systems Security Professional (CISSP) |
<table>
<thead>
<tr>
<th>EXPERT ID</th>
<th>YEARS of EXPERIENCE</th>
<th>PROFESSIONAL QUALIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert 2</td>
<td>6 years</td>
<td>Cisco Certified Security Professional (CCSP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Ethical Hacking (CEH)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Information Systems Security Professional (CISSP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Internet Web Security Analyst</td>
</tr>
<tr>
<td>Expert 3</td>
<td>7 years</td>
<td>Check Point Certified Security Administrator (CCSA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check Point Certified Security Expert (CCSE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Information Systems Security Professional (CISSP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Certified Security Professional (CCSP)</td>
</tr>
<tr>
<td>EXPERT ID</td>
<td>YEARS of EXPERIENCE</td>
<td>PROFESSIONAL QUALIFICATION</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Expert 4</td>
<td>6 years</td>
<td>Certified Information Systems Security Professional (CISSP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Systems Security Certified Practitioner (SSCP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Information System Auditor (CISA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Information Security Manager (CISM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified Ethical Hacking (CEH)</td>
</tr>
</tbody>
</table>

Their feedback was as follows.

A security expert from Kenya Revenue Authority stated that the separation of internal and external networks was very important. The concept brought out in the architecture where all traffic internal and external is treated as untrusted and therefore has to be scanned before forwarding to the desired destination is very important in ensuring information security. A point to highlight was that all network firewall should be next generation firewalls (NGFW) as opposed to traditional firewalls. This is because NGFW’s have better detection mechanisms including intrusion prevention system and detection of web attacks thus offering better security than the traditional firewall. However it was their proposal that there be a two sets of firewalls on for the internet edge and another for the datacenter which should manage all user access to local resources within the organization.
A security expert from the Information Communication Technology Authority (ICTA) Kenya stated that the architecture generally was good for infrastructure protection. However, it was highlighted that it would be important to have a load balancer to improve service delivery especially for resources that are used by customers as this will improve availability. It was also proposed that internal communication to servers should also be inspected as this will help deal with insider attacks as there will be visibility of user actions. This means introduction of an internal firewall. It was also proposed that server to server communication also be inspected as well but after careful consideration of any latencies that may be introduced due to forwarding all communication to the firewall first.

An information security expert from an IT solutions company Gestalt Gild, emphasized that the web application firewall and the database firewall are an important aspect in securing information. The need for a load balancer was also emphasized to ensure availability of services to customers. It was also proposed that a fraud detection and prevention system could be of use in a banking environment especially in an era where online shopping is on the rise. A fraud detection and prevention system enables detection and prevention of internal and external fraud.

A security expert form KCB Bank stated that, the architecture proposed was good for infrastructure protection. The WAF dynamic application profiling, granular policies, threat intelligence and report generation are very important in securing web applications. The DBF capability to identify sensitive data and system risks together with data classification and organization helps secure databases. The advanced capabilities of the WAF and DBF give better protection for application and databases than the NGFW’s. However it was noted that it is important to have the equipment especially security equipment in high availability for business continuity in case there is failure of on security equipment. The expert suggested integration of a Security Information and Event Management (SIEM) solution. This is important for easy visibility of the organizations
infrastructure security. The SIEM enables one to view all relevant data from a single point by collecting logs and security information from various devices. This makes it easy to identify issues and incidences.

4.5 Chapter Summary
An analysis of the current bank architectures indicates that the information infrastructure in banks is not adequately protected, the reasons why this is the cases is that there is not enough knowledge on how the systems ought to be protected, investment in security systems comes as an afterthought or is not paid proper attention to. There exists the notion that the network firewalls ability to have policies for network access control is enough to secure the organizations information. The proposed design has incorporated the use of WAF to protect the web applications and the use of DBF to protect databases together with network firewalls for intrusion detection all these features of the proposed architecture will help ensure confidentiality, integrity and availability, this will be discussed in the next chapter where effectiveness of the proposed architecture in IIP shall be the focus.
CHAPTER 5: RESULTS AND FINDINGS

5.1 Introduction

Information gathered from the interviews indicates that not much has been done to secure the information infrastructure in the banking institutions. There is a realization for the need to protect the information infrastructure but there inadequate protection mechanisms or system that have been put in place to ensure confidentiality, integrity and availability. As stated before, the network firewall is now not enough to protect institutions from the ever growing threat landscape, it used to be enough but with the revolution of IT and increase in online transactions with the aim of creating better services, attacks are also evolving and targeting web applications and databases.

This chapter shall focus at whether the proposed architecture is able to improve the Information Infrastructure Protection (IIP) of the banking institutions, focus shall be given on how the architecture will help in protecting the institutions information infrastructure against the advancing threat landscape.

5.2 Gaps in Information Infrastructure Protection for Banks

5.2.1 User Factor

Users are an important aspect of information security because they are the individuals that operate the various systems. Of the personnel interviewed, 6 out of 21 stated that they had no adequate technical know-how to enable them enforce IIP. The personnel who have done certifications that give them an information security background for instance technical certificates to enable firewall administration like CCNA (Cisco Certified Network Administrator) Security and CCSA (Checkpoint Certified Security Administrator) while others have CISA (Certified Information Systems Auditor) and CISM (Certified Information Security Manager) certifications which are focused on system audit and security management were 15. Despite that fact that 6 of those interviewed had no in-depth security knowledge, they have networking skills.
In this study the user who is the system administrator is a significant party in ensuring IIP because human beings have been said to be the weakest link in security. Human errors that are brought about by lack of skills on how to deal with information is what leads to security breaches in systems (Huang, Rau, & Salvendy, 2007).

Form the study carried out it was noted that having the adequate skills is important in IIP because without the skill required, the security personnel’s are not able to ensure IIP. This leaves the organization at a risk of being attacked without knowing what actions to take. The lack of security knowledge by the 6 information security personnel indicates a weak link in the protection of information infrastructure. With the proper skill one will know how to manage the security systems in place, identify system security requirements, analyze information, identify an attack and take necessary precaution to ensure protection.

**5.2.2 Security Threats**
Information security threats that were monitored across the four bank seemed to be similar as follows:

Viruses – A computer virus is a program that is configured to replicate itself across machines and infect computer files including programs and as a result affect the operation of a system. These viruses can be gotten from normal web activities through opening files with virus infected attachments, downloading and installing of software, accessing a site that has malware but to mention a few (Webroot, 2010).

Botnets – A botnet is a connection of devices which are infected and controlled by a common type of malware, these infected devices communicate with a command and control sever which is normally the attackers’ machine. A botnet scans systems and machines for vulnerabilities that can be exploited this includes firewalls or antivirus software (Rouse & Wright, Botnet, 2017).
DoS (Denial of Service) – This is a security event whereby an attacker prevents users from accessing computer systems, devices needed to carry out business functions. This attack sends traffic to the systems or devices in order to flood them and overwhelm system resources, making it difficult to use the systems (Rouse & Loshin, 2016).

5.2.3 Challenges in Ensuring IIP
All individuals involved in the interview process agreed that “there is need to improve the current information security infrastructure in order to better secure the systems from the always evolving security attacks”. However, this has not been possible as reported due to:

Budgetary constraints. The organization does not have the funds to purchase the security systems that are needed to improve the security of the various systems that are critical to banking operations.

The other challenge faced is that there is the assumption that a network firewall is enough to secure all information infrastructure in the network. Contrary to popular belief, the network firewall is not designed to detect database or web server attacks; therefore, the organization is still vulnerable to attacks that are targeted to the databased and web application servers.

Although the bank architectures have employed some sort of security measure, the security measures in terms of infrastructure do not offer the desired security. Despite the capability of firewalls to carry out intrusion prevention, the network firewall is not specifically built for this function. With the sophistication in attacks, it is important to have security mechanisms that are designed to protect the bank’s information infrastructure to offer the best security.

5.3 Effectiveness of the Proposed Architecture
The WAF technology comes with predefined rules but also allows for configuration of local policies which are used to prevent or allow contentions that match the criteria specified on the
policies. This can be based on the http requests that are processed, the http response and even number of occurrences. The policies can also be configured to match signatures and choose the action to be carried out. Figures below illustrate the policies configured on the WAF.

Web applications are designed to collect information through queries from a database, the web application security greatly depends on the database security. The DBF technology is able to carry audits on databases using audit policies that are preconfigured. It also allows for creation of policies for tables that are critical to the business such that an alert can be given when an operation like insert, select or delete is carried out.

Intrusion Prevention Systems (IPS) or Intrusion Detection Systems (IDS) technologies help in intrusion detection. This is a feature that is available on firewalls and there are also dedicated technologies for handling the same.

5.3.1 Synthesis of Expert Feedback

<table>
<thead>
<tr>
<th>Review Theme</th>
<th>Expert Feedback</th>
<th>Comment/ Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the network firewall enough for infrastructure protection.</td>
<td>The network firewall is important form infrastructure protection and must be present in any infrastructure. However just the network firewall is not adequate enough for information infrastructure protection, there is need to use other firewalls specific to applications and databases.</td>
<td>The proposed architecture has incorporated a web application firewall and a database firewall.</td>
</tr>
<tr>
<td>Review Theme</td>
<td>Expert Feedback</td>
<td>Comment/ Action</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Are the following infrastructures necessary in a bank; network, application and databases</td>
<td>Without the network infrastructure, there will be no communication, the application infrastructure allows bank customers to carry out online transactions while the databases store important customer information</td>
<td>The network, application and database infrastructure are clearly illustrated in the proposed architecture</td>
</tr>
<tr>
<td>How can protection of the application and database be achieved</td>
<td>The use of a Web Application Firewall (WAF) and a Database Firewall (DBF) will help in protection of the application and database against targeted attacks</td>
<td>The proposed architecture has a WAF and DBF to help protect against application and database targeted attacks</td>
</tr>
</tbody>
</table>

### 5.4 Chapter Summary

The proposed architecture is able to ensure that traffic from authorized sources is allowed while those from unauthorized sources are blocked. Attacks toward the web applications and databases can be blocked by the use of WAF and DBF since they are specifically designed to protect these infrastructures. With these security systems in place, there is improved information infrastructure is protected. A network firewall is not able to inspect http requests a responses or maintain web access signatures that are used to protect the web application from attacks. Therefore a WAF is very important to a bank because it ensures web application protection. A network firewall also does not have the capability of carrying out database audits based various database operations. The network firewall together with the WAF and DBF are able to ensure confidentiality, integrity and availability of information is maintained.
CHAPTER 6: DISCUSSION, CONCLUSION AND RECOMMENDATIONS

6.1 Introduction
The aim of this chapter is to discuss the findings of the study with support from literature then present the conclusions made from the results of analysis on the interviews and questionnaires satisfy the research objectives and finally make recommendations for further research.

6.2 Summary
The information infrastructure in the Kenyan banks consists of network devices which include router and switches, web servers and databases. The web servers are used to host web applications used by bank customers for activities like online banking. The databases carry tables that contain information used in various bank activities. This information includes and is not limited to customer details and bank account information. It is evident that attacks are constantly on the rise with hackers or attackers looking for new vulnerabilities in the evolving technologies.

With the use of mobile or online banking, the networks firewall is just not enough to secure the information infrastructure. Through the study, lack of skilled security personnel, lack of proper user awareness training, lack of the correct security measures in terms of infrastructure does not offer the desired security. Most organizations have the belief that a network firewall is able to protect against all attacks but this is not the case because it lacks the intelligence to analyze web applications and databases. The objective of this study was to come up with an architecture that will help improve the protection of a bank's information infrastructure.

Information on the current bank architecture was collected through interviews with information security personnel and it established that the information infrastructure in banks is not adequately protected. There are web servers accessible to the public that are protected by a network firewall which does not have the full functionality to protect against web application targeted attacks. The
proposed architecture offers better security for the information infrastructure as it aims to protect the critical banking infrastructure which is the network, web applications and databases.

**6.3 Discussion**

From the interviews carried out, one paramount challenge to information infrastructure protection is that there was an indication that the banking institutions security personnel are not fully skilled to help the banks ensure that the information infrastructure is protected. Due to the fact that some of the security personnel have no skill pertaining to security presents a problem.

As stated in the literature, to secure the information infrastructure, it is important to:

1. Have management support the security policies.
2. Have qualified security staff
3. Adhere to the security policies.
4. Train staff on security policy.
5. Have secure software development.
6. Have finance and insurance to cover the institution against losses.

The individual handling information security in an organization as sensitive as a bank must have the skill and knowledge as to be able to carry out their responsibilities satisfactorily. These institutions are working under the assumption that a network firewall is sufficient for all infrastructure protection. The question is in the event of an attack on the database or web application, what will be done?

The information security systems in place are not effective in detecting or preventing these attacks that are sophisticated and targeted to applications and databases. Without the three pillars of security in place there is no security enforced in an organization. Lack of interest in investing in security by top management is also a contributing factor to the lack of IIP in organizations. Most
organization think of security enforcement as an afterthought, they are not willing to invest in the security systems with the thought that they are not really necessary until the point where an attack occurs that is when there is a realization of the need to have the respective security systems.

An enterprise information security architecture should be holistic and should help in achieving the goals and mission of a business. This involves looking at the security requirements, processes, policies and information classification. The architecture should ensure that management of business functions is made easier by ensuring that development of the architecture is able to focus on the infrastructure being protected, factors how the same can be achieved and also what resources will be employed in ensuring information infrastructure protection. Ensuring that information security is achieved throughout the business structure is also important as suggested by SABSA in the model for security architecture.

Web vulnerabilities identified by various vulnerability classification bodies like CVE (Common Vulnerability and Exposure), WASC (Web Application Security Consortium) Threat Classification, OWASP (Open Web Application Security Project) and CWE (Common Weakness Enumeration) are injection, cross-site scripting lack of proper authentication, permission and access control, lack of encryption of sensitive data, cross-site request forgery just to mention a few.

To keep the web applications secure, a web application firewall is necessary. A WAF is a tool that is used to protect web applications and web application servers from attacks that are not able to be detected by a network firewall. A hacker is able to attack a web application even in the presence of a network firewall because, attacks aimed at the web application use methods like SQL injections, cross site scripting, command injections, cookie poisoning or session manipulation. A WAF is specific to web applications thus very useful in the application layer which is hosted on a
web server. The WAF allows for filtering of web traffic either positive, negative or session filtering (Khochare & Meshram, 2012).

Positive filtering works where communication is based on signatures that the system knows how to handle also known as whitelist, this prevents requests that are not know form reaching the web server. Session filtering allows for positive filtering and also allows for variables that are identified during sessions to be added to the whitelist.

However the use of positive filter has a disadvantage, to use only positive filter will require a large database of vulnerabilities so that all known web application functions or processes can be included, to fix this, WAF work as intelligent devices whereby they can learn the normal behavior then identify abnormal behavior together with detection modules for the different vulnerabilities (Kazanavicius, Kazanavicius, & A.Venckauskas, 2012).

The database is what contains the information that is used in banks. It is therefore important to ensure that the databases are secure. The database can be secured by analyzing query requests for any anomalies, this can be done by a database firewall (Bai & Liu, 2006).

Traffic to a database is first analyzed by the DBF the permitted to the database. The DBF is able to learn and identify normal queries from abnormal queries through the learning mode. In this mode, the firewall learns the access activities of a legitimate user where the firewall listens to queries from clients and records a script name of the query (Sun, Chen, & Niu, 2010).

Anomaly detection works by checking whether the query structure is recorded, if not, an anomaly score is calculated to measure to determine whether the query can cause any harm or not, then a decision to block or allow is made by the firewall (Sun, Chen, & Niu, 2010).
A network firewall is able to inspect traffic from internet connections and allow or block connections depending on the rules that have been put in place to manage access. A network firewall has intrusion detection and prevention features which will enable an organization know the intrusion that are detected in the organizations network and also gives the capability to block these intrusions (Lindstrom, 2004).

6.4 Conclusion

With the use of internet growing day by day, attacks are continually evolving the least an organization especially a banking institution can do is make sure that the information infrastructure that carries sensitive customer and business operations information is adequately protected. The IIP architectures that are currently in place indicate that banks are not secure, the banks may not let the public and customers know that they have been attacked but chances that the banks are losing money through cyber-attacks are very high.

The proposed architecture will significantly help reduce the number of attacks on web applications and databases because information security personnel in banks will be able to have the means to detect and prevent attacks targeted to the organizations’ systems. However acquiring the necessary systems is not enough; the security personnel equally need to be equipped with the skills that are necessary to carry out their jobs.

If an organization has the security systems in place but the personnel are not adequately trained to carry out any analysis on the attacks recorded and in turn give security recommendations to counter the attacks and prevent future attacks then the protections put in place are equally ineffective. Therefore with the constant change in technology and its operations constant training of the security personnel is very important and can never be ignored so that the personnel are competent enough to deal with the increasing risks.
6.5 Recommendation

The proposed architecture can significantly improve IIP however it is not final. For future studies, to further confirm that the architecture is functioning as described and meets the banking requirements, it will be best to look at the frameworks that have been put in place to ensure that commercial banking is operating in a manner that is acceptable by the banking governing body which is the Central Bank of Kenya. These various information security governance frameworks that are to be used in the banking industry these are FFIEC, COBIT, ISO27002 and PCIDSS. It will be important to ensure that apart from securing the banking infrastructure, the commercial banks are also adhering to the set frameworks that are designed to guide organizations to meet the requirements of a banking institution in a country.

The proposed architecture has been validated through expert feedback, for future work it will be important to look into development of policies and procedures that will help ensure the security mechanisms that have been put in place will serve their intended purpose and ensure infrastructure protection.
REFERENCES


Appendix I: Interview Questions for Discovery of the Current Architecture

In order to understand the current security architecture used in the banks involved in the survey, the following were the questions asked.

1) Do you have proper knowledge of your information infrastructure?
2) Do you have any certifications that are focused on information security?
3) Do you have the technical know how to manage the information security systems in place?
4) What are the threats you have monitored on your network?
5) Do you know the critical systems in your organization? Which are they?
6) Can you confidently say your information infrastructure is effectively protected?
7) What challenges do you face when it comes to ensuring IIP?
8) Give me a high level description of the information infrastructure
Appendix II: Interview Questions for Evaluation of the Proposed Architecture

The interview aimed to get a security expert review of the proposed multi-tiered architecture that can be used for information infrastructure protection in commercial banks. The study highlights the following as the most critical information infrastructure in commercial banks; Banks’ network infrastructure, Web application used for online/internet banking, Databases that contain core banking information like customer account information.

1) Is user awareness in an organization in this case a commercial bank important?
2) Is IT security personnel training important in an organization?
3) Is the network firewall adequate enough to protect all information infrastructure?
4) Are network infrastructures, application and database servers identified ideal for a bank?
5) Does the design have the capability to address the issue of web application and database attacks mitigation?
6) How effective do you think the design will be in the protection of information infrastructure?