IMPLEMENTATION OF PAYMENT CARD INDUSTRY DATA SECURITY STANDARD BY PAYMENT CARD COMPANIES IN KENYA: SURMOUNTING SECURITY CONCERNS

NAME: BWANA FLORENCE WEWEE

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION (MBA) SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

OCTOBER 2015

DECLARATION

I declare that this research proposal is my own account of my own research and has not been presented for examination before for the award of other degree or qualification in any university.

Signed_________________
Date________________

BWANA FLORENCE WEWEE

D61/61665/2010

The research project has been submitted for examination with my approval as the university supervisor.

Signed_______________
Date_________________

SUPERVISOR: DR. KATE LITONDO

LECTURER,

DEPARTMENT OF MANAGEMENT SCIENCE,

SCHOOL OF BUSINESS,

UNIVERSITY OF NAIROBI

ACKNOWLEDGEMENT

First, I thank the Almighty God for giving me life, courage and the ability to undertake this subject. This far I have come it's only through the grace of God. I wish to also thank my family and friends for their invaluable support.

Special thanks and gratitude to my supervisor, Dr. Litondo, whose guidance, advise and incredible support played a vital role in the compilation of this project. I also appreciate the entire staff in the MBA programme for their dedication and support towards the programme.

My heartfelt gratitude and appreciation goes to the management and staff at both Kenswitch Ltd and Paynet Ltd for giving me special consideration and participating in my research study. Their cooperation enabled me to successfully complete my MBA in Management Information System (MIS) studies.

DEDICATION

This project is dedicated to my late parents and brother, my brothers and sisters, and friends, for their patience, understanding, encouragement and prayers during this journey. Above all I thank God.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ATM – Automatic Teller Machine

PCI DSS - Payment Card Industry Data Security Standard

PCI SSC – Payment Card Industry Security Standards Council

PA DSS – Payment Application Data Security Standards

POS – Point of Sale

QSA –Qualified Security Assessors

TAM – Technology Acceptance Model

ABSTRACT

In the recent past, the Payment Card Industry has been riddled with cases of fraud. To counter this, or reduce the frequency of such occurrences, a worldwide accepted standard called Payment Card Industry Data Security Standard (PCI DSS) was introduced into the market. This study will establish the extent to which payment card companies have implemented PCI DSS compliance standard, determine the challenges of implementing PCI DSS Compliance and establish the relationship between PCI DSS compliance and card security concerns for Payment Card companies. Whereas some companies are compliant, some aren’t because of varied reasons as explained within the challenges aspect of this study. It is notable to add that this PCI DSS has been a challenge for many institutions to implement, and for those who have been able to implement, find it had to maintain the certification. Some of the challenges mentioned are lack of full stakeholder support, the business teams not being fully aware of the role they play in cards data security, the PCI DSS conditions seemingly looking overwhelming for most IT security practitioners, the implementation being seen as an expensive endeavour, and also the fact that a single violation of any of the conditions may lead an organization to being classified as non-compliance. Additionally, the study discusses the relationship between PCI DSS and card security where the findings show that the level of education of the organisation’s staff is critical to the security of card data in the Payment Card Company. Nonetheless, these challenges are surmountable, and Payment Card companies are highly encouraged to have card security as part of their organizational strategy.

CHAPTER ONE: INTRODUCTION

1.1 Background

There is a paradigm shift towards the frequent use of cards for payments instead of cash, and a lot of technological changes are taking place to change the way the payment card industry operates. History has also demonstrated that everything is dynamic, and that nothing is inevitable in this industry because even costs involved in implementations that bring innovation can, and would be recouped at any point. There have been technological developments involving online transactions, mobile transactions, wireless communications, industry specific software and analytics that have taken place within the industry that have allowed for patterns to be drawn so that relevant products that provide delightful customer experiences are developed (Schmalensee, 2009). Consequently customers' data needs to be protected technologically as well, and this is where the payment card industry data security standard (PCI DSS) comes in.

The payment card industry operates by use of cards. These are cards that are issued to an interested customer for use of purchase of either goods or services from retailers. These cards are usually plastic, embossed and conform to ISO/IEC 7812 standard of numbering in the payment card industry. The card number on the face of the card is usually linked to the customer's account number and their respective financial institutions which could either be a deposit or a credit account (Westpac Banking Corporation, 2011). Payment cards are differentiated by the features associated with each type of card. There are, debit cards, credit cards, prepaid cards etc. These cards are used electronically. The technologies commonly used to manufacture these cards are magnetic stripe cards, proximity cards or smart (chip) cards. It was noted that more than 1.2 billion credit cards are in use around the world, and accepted at more than 23 million locations. In 2003, credit cards were used in nearly 25 billion transactions totalling more than $2.3 trillion (MasterCard Worldwide, 2005). Therefore, the ecosystem within which these cards operate needs to be protected (see Appendix I).

Some of the challenges of implementing PCI DSS were found to be ensuring there is an organisation wide education and application of security around payment cards. Finding security loop holes in application systems before hackers exploit them was also another issue to contend with (McAfee for Business, 2015). Evaluating payment processing applications and products to meet the PCI DSS requirements of protecting cardholder data in transmission and at rest, and building a cost effective information security management system in the organization were also other challenges for organisations to have to deal with. Surmounting all these challenges, among others could sometimes prove to be very costly for some organisations to implement (First Data Corporation, 2009).

1.1.1 **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is the Payment Card Industry Data Security Standard, and this is a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. The way it does this is through tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. Initially, card companies developed their own policies (Xia, 2011). PCI DSS is intended to protect sensitive cardholder data (PCI Security Standards Council, 2010). The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS (see Appendix II) was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express (Acunetix, 2015). However, PCI DSS compliance doesn’t mean a system is completely immune from risk (E-Path, 2015).

When implementing PCI DSS for the first time, the changes in an organisation are major as it is an organisation wide standard, and this essentially means that capital expenditure is involved, usually high at most times. Also, often times, companies treat PCI DSS purely as compliance, and not as an on-going activity which leaves room for card security breaches. Additionally, companies appeared to have particular problems with PCI requirements in protecting data at rest (Vijayan, 2014).

1.1.2 **Data Security**

Data security refers to all the measures applied to ensure that databases are not accessed by unauthorised people (Techopedia, 2015). These measures that are applied could be like data encryption techniques, data masking and data scrambling. Data security is also about ensuring the availability, confidentiality and integrity of the data (Himma, 2007). When the contrary occurs to personal data, and the data is compromised, this action is then called a breach which could lead to either a loss or unauthorised disclosure (Paul De Hert, 2010).

Fraud has been experienced in one way or another in the payment card industry, and this could be either with the card by way of a skimmed card or by way of intercepting and re-routing transactions while they are in transit. This then means that payment card ecosystem needs to be fool proof so as to protect the consumer against fraud (Rouse, 2009), and this is the concern that this paper was based on.

Security matters are extremely important. It was found that the IT department is responsible for the processing of data, but the ultimate responsibility for application systems rested with the user departments served by them (French, 1996). French went on to say that a complete IT policy must be evolved and applied and that it could only be fully exploited by people who have the requisite knowledge and experience.

Protecting card holder data is very critical for any company because the repercussions of not doing so are very grave. Payment card data remains very lucrative because of its ease of conversion to cash, and thus PCI DSS becomes the standard by which the payment card industry is governed by to protect itself. (Verizon, 2014).

1.1.3 Payment Card Companies

In Kenya, we have two payment card companies. That is, Paynet Ltd and Kenswitch Ltd. Launched in 2003, Paynet currently services customers in Kenya, Uganda, Tanzania and Rwanda and it is an African based organisation. Paynet Group comprises of three strong East African brands, Paynet, PesaPoint and Electronic Financial Technologies (EFT). The Group is a mature and respected provider of E-Banking services and solutions to the financial sector within the region and prides itself in delivering value added products and services to its customers through continuously innovating and providing solutions that enhance efficiencies (Paynet Ltd, 2014).

Kenswitch is a registered limited company that was set up by a consortium of banks under the National Payments Systems modernisation and reform process of the Central Bank of Kenya. Its terms of reference are to allow participating financial institutions to share payment infrastructure like Automated Teller Machines (ATMs) and Point of Sale (POS) terminals so as to avoid the duplication of scarce resources (Kenswitch Ltd, 2014).

1.1.4 Statement of the Problem

In the recent past, there has been increasingly more reports on card systems being hacked into, accounts being hacked and funds siphoned, cards being skimmed and huge losses and frustrations are meted on both the company and the customer. Protecting the cardholder information from its raw state; all the way to the final transaction posting stage is critical for an organisation to survive in this competitive world. The organization that can mitigate against this risk gets a competitive edge. This is because the fear of possible fraud drives customers and potential customers away (Landon, 2007).

According to a study by Verizon (2009), in the case study of the US based company called Target Group, 81% of the companies were found not compliant with PCI DSS or had never been audited. This status was determined by the victims' attestations or Qualified Security Assessors (QSA). In 66% of the cases, the breaches involved data that the organization didn't even they know they had (Verizon, 2009). Additionally, fraudulent use of stolen card data was confirmed in 83% of Verizon's cases and 91% of all compromised records were linked to organized criminal groups. A survey by Gartner (2008), it was discovered that the implementation and ongoing maintenance of the needed technology measures was expensive, and it continues to grow more expensive with time (Gartner, 2008). In the same report, it was also reported that some retailers reported spending an average of $2.7 million on PCI compliance, excluding the costs of PCI assessment services. Further, PCI DSS compliance is supposed to be maintained continuously.

In November 2014, Paynet Ltd reported to having gained PCI DSS certification, and becoming one of the first companies in East Africa to achieve this compliance standard. Their company CEO, Bernard Mathewman, is reported to having welcomed other players in the payment card industry in the East Africa region to join their network since they have already been certified. He described the compliance project as being very complex and rigorous because it required new versions of hardware, software and tools at every stage, alongside about 350 new processes and procedures (Paynet, 2014). This goes to show that PCI DSS compliance is indeed possible to achieve. For any business that comes into contact with card data, PCI DSS is the standard that is most comprehensive for card security (Jefwa, 2015). 3G Direct Pay Ltd is another company that operates within the East Africa region that has managed to achieve PCI DSS compliance. As a merchant, for a large part of compliance they had to show evidence of all controls implemented in order for them to be certified. All merchants should verify that their payment service provider and their payment gateways are PCI DSS compliant, and in cases when they are not, they should be put to task to give the timelines to becoming compliant which takes roughly 18 months of rigorous effort else theirs become a risky platform for card consumers to use (Jefwa, 2015).

With the incredible growth towards globalisation of economies, standardisation through compliance certifications seems to be the new normal as this becomes the benchmark upon which organisations are marked with the most popular certification in Kenya being the ISO 9001 certification for Quality Management Systems (Omukhweso, 2012).The most notable information security management system (ISMS) standard is ISO 27001:2013 or the 27000-series which checks adequately security controls and is internationally recognised (Kenya Bureau of Standards, 2014) used in all kinds of organisations in all sectors. However, this is not enough for an organisation that deals with card data, and thus and organisation would have to also incorporate PCI DSS to become more fool proof and protect their customers.

They are compatible (27001 Academy, 2014).This is the gap left out in the scope by ISO 27000 series and it is best filled with PCI DSS. In as much as PCI DSS wasn't meant to match ISO 27000 series, it clearly is not set far apart in terms of its security concern (IT Governance, 2003-2015).

1.2 Objective of the Study

a) Establish the extent to which payment card companies have implemented PCI DSS compliance standard

b) Determine the challenges of implementing PCI DSS Compliance

c) Establish the relationship between PCI DSS compliance and card security concerns for Payment Card companies

1.3 Value of the Study

This study will offer value to financial institutions in that they will get to understand what PCI DSS can accomplish for an organisation and use it to their advantage as a competitive edge when they maintain their commitment to it. Maintaining a state of continuous compliance requires focused effort and coordination, thus organizations accustomed to traditional approaches to PCI DSS compliance that focus primarily on annual validation may find it difficult to build in the people, processes, and technology necessary to support sustained compliance. Executive sponsorship is critical if organizations want to be successful in implementing ongoing PCI DSS compliance programs (PCI Security Standards Council, 2014).

Policy developers will be able to use this study to build framework around payment card security. Also, there are numerous governance frameworks available that can be used to complement PCI DSS controls to enhance the overall effectiveness of an organization's cardholder data security program (PCI Security Standards Council, 2014). Additionally, this paper can also be used for academic purposes as it contributes to the research body of knowledge that already exists.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter will be offering more information on card data security in the Payment Card Industry. It will also discuss card data security, as well as offer more understanding on the implementation of the PCI DSS standard and the challenges that accompany its implementation. Additionally, some empirical studies already done will be discussed as well as the theoretical foundations of the study.

2.2 Payment Card Industry

PCI DSS standards came about in 2004, along with the PCI Security Council. The payment card industry is rapidly changing, fuelled by technological advances in software, systems and hardware. Along with this growth has come a surge in technological crimes, leading to more strict and more complex standards for anyone who stores, transmits, or processes payment card data to adhere to. The primary goal of PCI is aimed at reducing the risk of transaction and raising awareness of key aspects of data security (Xia, 2011). High-profile data losses have led to the development of the Payment Card Industry Data Security Standard (PCI DSS), originally created by Visa, MasterCard, Discover and American Express, to protect cardholder information and reduce data theft. The PCI DSS certification consists of security requirements for any organization that comes in contact with payment card data. The payment brands (Visa, MasterCard, Discover, American Express and JCB) enforce compliance with the PCI DSS for member banks, merchants, and service providers they partner with. Transaction information that is maintained must be safeguarded according to stringent guidelines. By becoming PCI DSS compliant, merchants protect customers from losing valuable card data and insulate themselves from possible legal action and certain fines from the payment brands like Visa and MasterCard’s chargebacks (Chiu, 2011).

2.3 Card Data Security

PCI Security Standards Council (PCI SSC) (2010) states that the Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and it facilitates the broad adoption of consistent data security measures globally, across all payment card companies. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – and this is including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (MasterCard Worldwide, 2005).

For any installed applications running along within the payment card company’s ecosystem, there exists compliance as well. Running of software applications must adhere to the spin off that is Payment Application Data Security Standards (PA DSS). The PA DSS was developed by the PCI SSC to ensure that software vendors and others who develop payment card applications that store, process and/or transmits cardholder data allow the environment in which it is implemented to be compliant to the PCI DSS (Westpac Banking Corporation, 2011).

The PCI Security Standards Council contends that merchant-based vulnerabilities may appear almost anywhere in the card processing ecosystem. This includes automatic teller machines (ATM), point-of-sale (POS) devices, personal computers or servers, wireless hot spots, Web-based shopping applications, storage systems and the unsecured transmission of cardholder data to service providers. Susceptibilities also can extend to outside systems operated by service providers and acquirers. These vulnerabilities can, and often do, lead to the exposure or theft of sensitive cardholder data, especially at the merchant level. The Verizon business risk team reports that payment card breaches were at the top of the list of all reported data breaches in 2008, which even outnumbered other data-type breaches. Additionally, fraudulent use of stolen card data was confirmed in 83% of the breach cases investigated by the Verizon team (Verizon, 2009).

2.4 Implementation of PCI DSS Standard

Bendigo and Adelaide reported that by minimising the risk of data compromise, implementation of PCI DSS assists businesses to protect against potential financial liabilities, investigative costs and the risk of invasive media attention (Bendigo and Adelaide Bank, 2006).

There are 12 requirements in PCI DSS (see Appendix II) and they are grouped into 5 key areas to ensure transaction and cardholder data is secured. These are; building and maintaining a secure network (requirement 1 – 4), maintaining a vulnerability management programme (requirements 5 – 6), implementing strong access control measures (requirements 7 – 9), regularly monitoring and testing networks, (requirements 10 – 11) and maintaining an information security policy (requirement 12) (Dimension Data, 2011).

As the first step, it is very important to build a strategy to determine your existing status and future goals; because the requirements on the different merchants and payment card companies and provider levels will affect your approach to the project.

The second step is to assess performance and risk of the organisation. Organisations need to conduct a thorough assessment of where personal account data is held. They need to understand where their weaknesses exist, and how they need to be addressed. Without conducting this assessment, virtually all payment card companies will be reactive in their data security practice.

Thirdly, once assessments have taken place, organisations need to build an architecture that supports the overall IT security and compliance roadmap. This often includes re-architecting the existing network and security controls to create architecture that can address changes in the 12 requirements outlined.

Fourth, an organisation is advised to not store what they do not need as the golden rule for data security avoidance. When there is need to store data, an organisation is advised to develop appropriate storage, retrieval and disposal processes. Additionally, businesses need to become more systematic in the destruction of transactional data once the business purpose for keeping it has passed.

Fifth, intrusion detection tests and audit trails are paramount in protection of the security perimeter of the organisation. Organisations are advised to proactively monitor and manage the network. While larger organisations seem to be more focused on ensuring that sensitive data remains secure throughout the life cycle of business applications, businesses of all sizes find tracking and monitoring a major business challenge. This can be mitigated by enacting clear policies of network administration.

2.4.1 Challenges of Implementing PCI DSS

While adoption of PCI DSS has improved steadily over the years, industry reports highlight the challenge of ongoing maintenance of PCI DSS controls as part of a daily business process, with organizations often viewing PCI DSS compliance as an annual event and unaware that compliance needs to have an all year round continuous focus. Building a culture of continuous security and vigilance is vital to meet the intent of the PCI DSS, which is safeguarding payment card data at all times (PCI Security Standards Council, 2010).

In his article, O'Neill (O'neill, 2015) says that given the evolution of security threats, network penetration testing is more important than ever. He said that the difficulty was in the details. These penetration tests must comply with recognized industry standard testing methodologies. The tests continuously look out for intrusions into cardholder environment.

PCI DSS Compliance is very expensive. According to a 2008 survey by Gartner Inc., Level 1 (see Appendix III) retailers reported spending an average of $2.7 million on PCI compliance, excluding the costs of PCI assessment services. That number compares with an average of $568,000 reported by Level 1 merchants in a 2006 Gartner survey. Similarly, Level 2 merchants reported spending $1.1 million on PCI compliance, as opposed to an average spending of $267,000 reported in 2006. Altogether, Level 1 and Level 2 U.S. merchants' spending to protect cardholder data and become PCI compliant increased nearly fivefold within a short time, still according to the Gartner report. Despite the expenditures, many Level 1 and Level 2 companies are still struggling with PCI and are coming to realize that the cost of PCI compliance is much underestimated.

Although the DSS is clearly structured, there is no doubt that organisations may find it challenging to interpret how they match their overall security roadmap and also previous investments in technology and processes. A single violation of any of the requirements can trigger an overall non-compliant status resulting in fines, suspension and revocation of card processing privileges (Pennington, 2011).

2.5 Empirical Studies on Card Payments and Data Security

Addressing security concerns around current and emerging payments systems isn’t the job of a single company or stakeholder (Ponemon Institute, 2009). Payment card companies have a lot of personal data elements that need to be protected. Throughout their study, they found that a large percentage of companies are likely to keep moving forward with deployment of new technologies despite concerns about security.

Only 16 % of their respondents felt companies were very effective in responding to breaches, thus there is a lot of room for improvement in that area. On security, 69% of the respondents said that highly publicized data breaches did increase their awareness about securing their payment processes and systems. However, 50% of respondents mentioned that they were not confident in the security of emerging payment systems. An interesting element worth mentioning is that the greatest vulnerability is in online purchases. 34% of respondents confirmed this. 25% was reported for both points of sale and mobile payments. 47% of respondents rate their security posture in dealing with these risks as only somewhat effective, 25 % of respondents or not effective (Ponemon Institute, 2009).

Another important factor to consider is checking the customer convenience versus security in the new payment ecosystem; the most likely innovations to increase the risk of a data breach are virtual currencies, mobile payments and near field communications. 66% strongly agreed and agreed that authentication risks made it difficult to implement new payment methods and

68% say the pressure to migrate to new payment systems can exacerbate the security risk (Ponemon Institute, 2009).

On the risk of data breach in the new payment systems, 75% of respondents said the company that loses customer information should do the most to protect lost customer information. Banks that issued the payment cards involved in the breach should also be involved. According to 69% of respondents only 35% of respondents say they are confident that customers have the tools and resources to protect themselves following a data breach event that resulted in the loss or theft of their personal information (Ponemon Institute, 2009).

In November and December of 2013, cybercriminals breached the data security of Target, one of the largest U.S. retail chains, stealing the personal and financial information of millions of customers. This was the largest breach in the history of United States. To date, Target has reported data breach costs of $248 million. Loss of customers, fines from other financial institutions were not even included in that amount. The industry can agree on one thing, that there is a need for action in matters related to card data security (Miller, 2015).

2.6 Theoretical Foundation of the Study

Theories help us put things into perspective. For instance, Chaos theory studies seek to identify patterns in behaviour over the long term and it is a part of the complexity theories. This theory can be defined as the qualitative study of unstable periodic behaviour in deterministic non-linear dynamical systems (Kellert, 1993). It deals with systems whose behavioural patterns are not predictable or always repeatable. Chaotic systems are deterministic in that, given the initial conditions; there is one unique end point or goal of the system that can be mathematically derived. Small changes in the initial conditions may generate very different end points. Nonetheless, deterministic doesn’t imply total predictability (Tsoukas, 1998). The payment card systems may be fully installed and configured initially, but these configurations will definitely have to be fool proof and go through necessary changes, and this dynamism due to system threats or occurrences, causes the systems in payment card companies to be complex. In many systems, the complexity is magnified as there is constant intervention involving new conditions and environmental change. Such a level of complexity may be impossible to fully explain and predict with limited human understanding, and simulations would be impossible to build, given the limits of computer technology (Kellert, 1993).

Another theory, Systems theory, is an interdisciplinary theory about every system in nature, in society and in many scientific domains as well as a framework with which we can investigate phenomena with a holistic approach (Capra, 1997). Systems thinking comes from the shift in attention from the part to the whole (Checkland, 1997), considering the observed reality as an integrated and interacting collection of phenomena where the individual properties of the single parts become indistinct. This is to confirm that a payment card's transactions' card system doesn't exist in isolation but as part of a system, and thus increases its complexity in terms of operations and also add on the human perspective of handling systems. Thus, systems have to work in a harmonious relationship towards a common goal. The PCI DSS compliance embraces this theory to the extent to which it puts checks in all systems that are involved in card holder data environment.

Technology acceptance model (TAM) provides a basis upon which one traces how external variables influence belief, attitude, and intention to use (Davis, 1989). According to technology acceptance model, ease of use and perceived usefulness are the most important determinants of actual system use. Directly applying this theory to this research topic, it fits perfectly. PCI DSS deals with organisation change and this change needs to be accepted in equal measure by all for it to be a success.

2.7 Summary of Literature Review

The ecosystem of the payment card industry is very dynamic due technological advancement that seems to be moving rapidly. Therefore, all matters regarding the security needs to advance at an equal pace. From the PCI council, it is noted that the PCI DSS requirements have a tremendous impact on the information technology systems utilized by every company in the card processing ecosystem.

Compliance efforts have forced merchants to update existing systems and implement new hardware and software in order to segment networks, install firewalls, deploy data encryption technologies, implement data access controls, track and monitor access to data and networks, and much more. In as much as this implementation of PCI DSS is necessary, it does come with challenges. As reported within the Payment Card Industry, the compliance areas are overwhelmingly many and thus the costs associated with implementing PCI DSS is very high, especially more that it needs to be continuously maintained by an organisation as opposed to it being an annual activity. Moreover, the users within the ecosystem need to be trained in all the details that go into compliance.

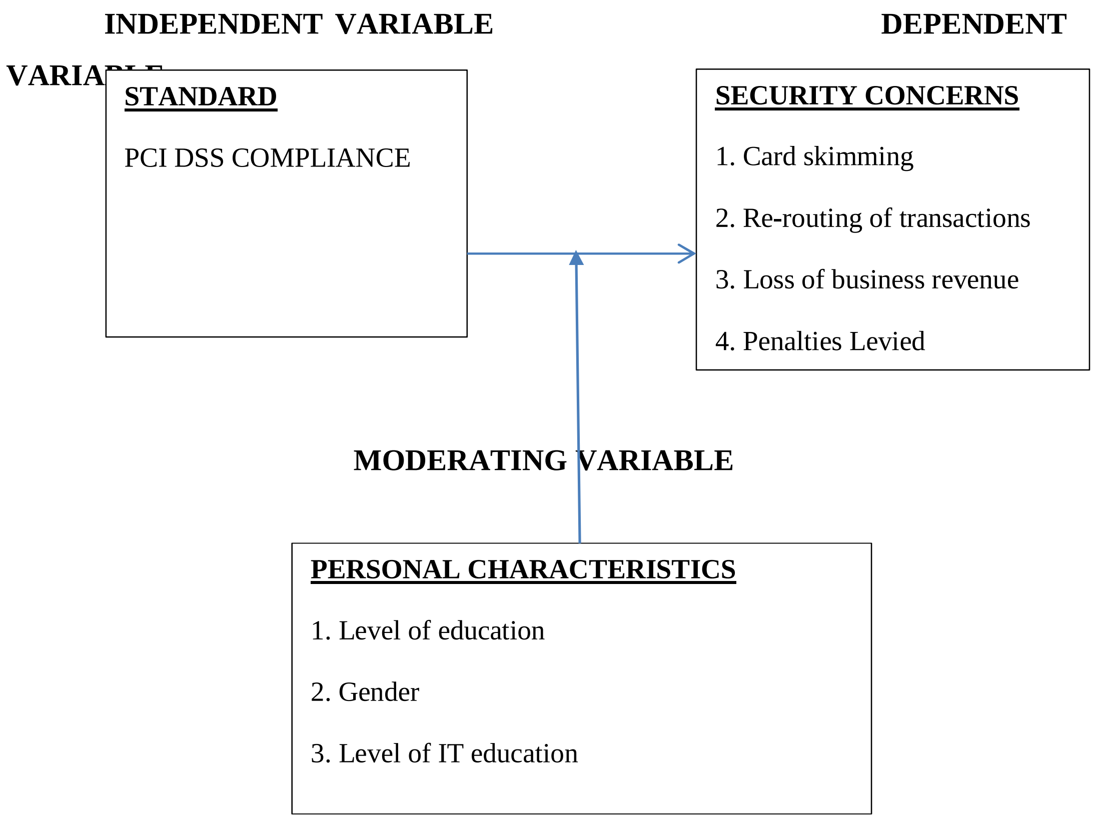
The empirical studies reveal that addressing security concerns is not the job of a single stakeholder, but rather an industry wide endeavour. This is because a single point of failure affects many within the Payment Card Industry ecosystem; therefore all are encouraged to get compliant with PCI DSS. The theoretical foundations were also explained. For this study, one of the associated theories is the Chaos theory where it is explained that complexity is magnified when there is a lot of exposure to dynamism. Another theory mentioned was the Systems theory which impresses upon the need to view systems holistically as opposed to individual units. Last but not least, the Technology Acceptance Theory was explained where ease of use for any new technological advancement made is incredibly important for its success.

In conclusion, it is critical that Payment Card companies maintain an ecosystem that is compliant with PCI DSS global standard going forward, and should also make it a top priority to reduce data breach occurrences. Additionally, it is notable that there is a paradigm shift towards consumers opting to use cards to do more transactions in more instances due to the convenience that cards offer, hence making the risks related to card data breach potentially go higher in future. The threats are real.

2.8 Conceptual Framework

Security concerns depend on compliance with the PCI DSS standards. However, personal characteristics of the employees can also have an effect on security concerns and are therefore termed as the moderating variable.

Figure 2.8 Conceptual Framework



Source: Own contribution (2015)

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter will describe the methods and procedures that will be used to conduct the study in order to achieve the objectives. It will provide details on the research design, study population, data collection and data analysis.

3.2 Research Design

A census survey was conducted for the study. In census survey research, the researcher collects responses from the entire population.

3.3 Study Population

The target population was all the payment card companies in Kenya for this study, the researcher collected responses from all the payment card companies operating in Kenya.

3.4 Data Collection

The study collected primary data from the respondents. The target respondents were the technical and operations department teams. This was because they have the experience and knowledge on PCI DSS compliance and interact with the ecosystem on a regular basis and relate to it. This formed the sample of 40 respondents who formed the sample respondents for this study. This study adopted stratified sampling technique to identify the respondents from the payment card companies in Kenya. This is where the population is divided into different groups called strata that more homogenous when alone than when it is the total population (Kothari, 2004). This was because the results were to be more accurate and reliable.

Questionnaires were used to collect the data, and they were administered electronically. The questionnaire comprised of the three objectives. Objective (a) and (b) which was covered under section A and B. Objective (b) which was covered in section C, while objective (c) was covered under section D.

3.5 Data Analysis

Data related to objectives (a) and (b) was analysed using descriptive statistics which summarised the set of data (Kothari, 2004), while data related to objective (c) was analysed using the following regression model:

$$Y=a_0 +a_1x_1 +a_2x_2+e$$

Whereby;

Y=security concerns

x_1=PCI DSS Compliance

x_2=Personal characteristics

a_0, a_1, a_2 are the parameters to be estimated or regression coefficients

e is the error term

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter covers statistical data analysis using SPSS software, results and discussions of the research. Data was summarised by means of statistical averages and presented in the form of tables. Out of 40 questionnaires, 34 were completed and returned, thus representing a response rate of 85% which was considered satisfactory for analysis.

4.2 Distribution of Respondents by their Level of Education and Gender

The respondents were asked general questions on demographics, and the results are as shown in the table below. The table shows the characteristics of respondents by their level of education and gender. From the table, majority of the respondents have university bachelor’s degree level of education at 88.2 % of the total respondents, with male respondents being majority with bachelor’s degree at 61.8 % of the total respondents. This showed that majority of respondents have better education to understand their work environment very well.

Table 4.2 General Demographics

		Gender of Respondent		Total
		Male	Female	
The Level of Education of the Respondent	College certificate	2(5.9%)	0(0.0%)	2(5.9%)
	College Diploma	1(2.9%)	1(2.9%)	2(5.9%)
	Bachelor Degree	21(61.8%)	9(26.5%)	30(88. %)

Total	Total	24(70.6%)	10(29.4)	34(100%)

Source: Research Data (2015)

4.3 The Extent of PCI DSS Compliance in Payment Card Companies in Kenya

The extent to which payment card companies have implemented PCI DSS compliance standard was measured by use of variables that required a respondent to rate their perception on PCI DSS compliance on 9 variables by 'Strongly agreeing' 'Agree' Neutral' 'Disagree' 'Strongly disagree'. Tables and analysis that follow below show description on how the respondents rated their perception on PCI DSS compliance in their companies. Responses were coded and given numerical values as follows: *Strongly Agreed=5; Agreed=4; Neutral=3; Disagreed=2; Strongly Disagreed=1.*

4.3.1 Analysis to Establish the Extent to which Payment Card Companies have Implemented PCI DSS Compliance Standard

In this analysis I used *percentages or proportions*, *mean* and *standard deviations* as parameters for descriptive statistics. From the table, we could see that 50 percent of the respondents either 'strongly disagreed 'or 'disagreed' that PCI DSS is too hard to implement. We could also see that the mean value of responses was 2.69 and a standard deviation of 0.946.With a mean value of 2.69 and standard deviation of 0.946 it shows that the responses tended more towards '*neutral*' on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean as parameter to measure the respondents perception on whether PCI DSS is hard to implement.

These results indicate that the respondents do not find PCI DSS compliance hard to implement as 44.1 % disagreed with the statement that PCI DSS is too hard to implement.

Table 4.3.1 Distribution of Respondents by whether PCI DSS is too hard

Type of response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongy Disagree	2	5.9	5.9	5.9

Disagree	15	44.1	44.1	50
Neutral	10	29.4	29.4	79.4
Agree	6	17.6	17.6	97.1
Strongly Agree	1	2.9	2.9	100
Total	34	100	100	

Mean =2.69, Standard deviation=0.946, n=34, Source: Research Data (2015)

4.3.2 Analysis of whether PCI DSS is Unreasonable and requires too much time

The table below describes the perception of respondents on whether PCI DSS is unreasonable and requires too much time to implement. From the table 82.2% of the respondents either ‘Strongly disagreed’ or ‘disagreed’ that PCI DSS is unreasonable and requires too much time to implement. The mean value of responses was 1.94 and a standard deviation of 0.866.With a mean value of 1.94 and standard deviation of 0.866 it shows that the responses tended more towards ‘*Disagree*’ on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean as parameter to measure the respondents perception on whether PCI DSS is unreasonable and requires too much time to implement.

A total of 11.8% respondents agreed that PCI DSS required too much time to implement, whereas a total of 58% disagreed. This results go to show that with proper planning for this compliance the time consumed in doing it is not viewed as too much by a majority.

Table 4.3.2 Distribution of Respondents by whether PCI DSS is unreasonable and requires too much time

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	10	29.4	29.4	29.4
Disagree	20	58.8	58.8	88.2
Agree	4	11.8	11.8	100.0
Total	34	100.0	100.0	

Mean =1.94, Standard deviation=0.866, n=34, Source: Research Data (2015)

4.3.3 Distribution of Respondents by Quantity of Card Transactions for one to be Compliant

The table below describes the perception of respondents on quantity of card transactions to be compliant. From the table, 82.4 % of the respondents either '*Strongly disagreed'* or *'Disagreed'* that their companies do not have a lot of card transactions to be compliant. The mean value of responses was 1.79 and a standard deviation of 0.880.With a mean value of 1.79 and standard deviation of 0.88 it shows that the responses tended more towards '*Disagree*' on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean as parameter to measure the respondents perception that their companies do not have a lot of card transactions to be compliant.

The data 44.1% below depicts the fact that it doesn't matter the quantity of card data a Payment Card Company hosts, PCI DSS compliance is necessary for all Payment Card Companies.

Table 4.3.3 Distribution of Respondents by Quantity of Card Transactions for one to be Compliant

Type of response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	15	44.1	44.1	44.1
Disagree	13	38.2	38.2	82.4
Neutral	4	11.8	11.8	94.1
Agree	2	5.9	5.9	100.0
Total	34	100.0	100.0	

Mean =1.79, Standard deviation=0.880, n=34, Source: Research Data (2015)

4.3.4 Distribution of Respondents by whether PCI DSS makes Organizations Store Card Data

The table describes the perception of respondents on whether PCI DSS makes organizations store card data. From the table below, 29.4% of the respondents 'Strongly disagreed', 17.6% 'disagreed', 14.7% had 'neutral' perception. Cumulatively at 61.8 percent of the respondents either 'strongly disagreed', 'Disagreed' or had 'neutral' perception towards whether PCI DSS makes organizations store data. The mean value of responses was 2.82 and a standard deviation of 0.1.55.With a mean value of 2.82 and standard deviation of 1.55 it shows that the responses tended more towards ‘Neutral’ on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean.

The research results from the respondents 47% disagreed with the statement that PCI DSS makes organisations store card data. The fact that also 14.7% were neutral also tends to show that data storage by Payment Card Companies cannot be avoided, a thus stringent security measures need to be implemented, by the use of PCI DSS compliance.

Table 4.3.4 Distribution of Respondents by whether PCI DSS makes Organizations Store Card Data

Type of response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	10	29.4	29.4	29.4
Disagree	6	17.6	17.6	47.1
Neutral	5	14.7	14.7	61.8
Agree	6	17.6	17.6	79.4
Strongly Agree	7	20.6	20.6	100.0
Total	34	100.0	100.0	

Mean =2.82, Standard deviation=1.55, n=34, Source: Research Data (2015)

4.3.5 Distribution of Respondents by whether PCI DSS makes their Companies more Secure

The table below describes the perception of respondents on whether PCI DSS makes whether PCI DSS makes companies secure. The mean value of responses was 3.94 and a standard deviation of 1.36. The mean value of 3.94 and standard deviation of 1.36 shows that the responses tended more towards ‘Agreed’ on a Likert scale, and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean.

From the table 47.1% of the respondents either ‘Strongly Agreed’, 32.4% ‘Agreed’ with the perception that PCI DSS makes companies secure.

Essentially, this is to prove that PCI DSS compliance is a necessity to any Payment Card Company.

Table 4.3.5 Distribution of Respondents by whether PCI DSS makes their Companies more Secure

Type of response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	4	11.8	11.8	11.8
Disagree	2	5.9	5.9	17.6
Neutral	1	2.9	2.9	20.6
Agree	11	32.4	32.4	52.9
Strongly Agree	16	47.1	47.1	100.0
Total	34	100.0	100.0	

Mean =3.94, Standard deviation=1.36, n=34, Source: Research Data (2015)

4.3.6 Distribution of Respondents by whether PCI DSS Compliance is an IT Project

The table below describes the perception of respondents on whether PCI DSS compliance is an IT project or not. From the table, commutatively 50% of the respondents either 'Strongly Disagreed' or 'Disagreed' with the perception that whether PCI DSS compliance is an IT project. The mean value of responses was 2.85 and a standard deviation of 1.46. The mean value of 2.86 and standard deviation of 1.46 shows that the responses tended more towards 'Neutral' on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean.

As noted below, 29.4% agree that PCI DSS compliance is and IT project. However, 23% tend to strongly differ with the statement. These are the respondents who believe the compliance is an organization wide affair because in as much the technology around PCI DSS will be implemented, there will have to be people who operate within its confines.

Table 4.3.6 Distribution of Respondents by whether PCI DSS Compliance is an IT Project

Type of response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	8	23.5	23.5	23.5
Disagree	9	26.5	26.5	50.0
Neutral	2	5.9	5.9	55.9
Agree	10	29.4	29.4	85.3
Strongly Agree	5	14.7	14.7	100.0
Total	34	100.0	100.0	

Mean =2.85, Standard deviation=1.46, n=34, Source: Research Data (2015)

4.3.7 Distribution of Respondents by whether one Vendor can make an Organization PCI DSS compliant

The table below describes the perception of respondents on whether one vendor can make an organizations PCI DSS compliant. From the table, commutatively 61.8% of the respondents either ‘Strongly Disagreed’ or ‘Disagreed’ with the perception that one vendor can make an organizations PCI DSS compliant. The mean value of responses was 2.50 and a standard deviation of 1.21. The mean value of 2.50 and standard deviation of 1.21 shows that the responses tended more towards ‘Neutral’ on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean.

Additionally, from the research results, 17.6 % and 44.1% of the respondents strongly disagreed and disagreed, respectively, that not one vendor can make an organization PCI DSS compliant.

Table 4.3.7 Distribution of Respondents by whether one Vendor can make an Organization PCI DSS compliant

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	6	17.6	17.6	17.6
Disagree	15	44.1	44.1	61.8
Neutral	7	20.6	20.6	82.4
Agree	2	5.9	5.9	88.2
Strongly Agree	4	11.8	11.8	100
Total	34	100	100	

Mean =2.50, Standard deviation=1.21, n=34, Source: Research Data (2015)

4.3.8 Distribution of Respondents by whether Outsourcing Card Processing makes an Organization PCI DSS Compliant

The table below describes the perception of respondents on whether outsourcing card processing makes an organization PCI DSS compliant. From the table, commutatively 64.7% of the respondents either 'Strongly Disagreed' or 'Disagreed' with the perception that one vendor can make an organizations PCI DSS compliant. The mean value of responses was 2.50 and a standard deviation of 1.21. The mean value of 2.24 and standard deviation of 1.07 shows that the responses tended more towards 'Disagree' on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean.

From the respondents' responses, it was found that 29.4% strongly disagreed, and 35.3% disagreed with the statement that outsourcing card processing can make an organization PCI DSS compliant. This is true because, for all transactions that take place, there will either be data at rest, or data in transmission states, and thus data protection cannot be wholly handed over to a third party to manage it security. Security remains paramount to all Payment Card Companies.

Table 4.3.8 Distribution of Respondents by whether Outsourcing Card Processing makes an Organization PCI DSS Compliant

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	10	29.4	29.4	29.4
Disagree	12	35.3	35.3	64.7
Neutral	6	17.6	17.6	82.4
Agree	6	17.6	17.6	100.0
Total	34	100.0	100.0	

Mean =2.24, Standard deviation=1.07, n=34, Source: Research Data (2015)

4.3.9 Distribution of Respondents by whether a Completed Self-assessment Questionnaire (SAQ) makes one PCI DSS Compliant

The table below describes the perception of respondents on whether completed a self-assessment questionnaire (SAQ) makes their companies PCI DSS compliant. From the table, commutatively 76.5% of the respondents either 'Strongly Disagreed' or 'Disagreed' with the perception that completed a self-assessment questionnaire (SAQ) makes their companies PCI DSS compliant. The mean value of responses was 2.50 and a standard deviation of 1.21. The mean value of 2.06 and standard deviation of 0.74 shows that the responses tended more towards 'Disagree' on a Likert scale and dispersion of responses from the mean was within agreeable limit respectively i.e. the data is well spread towards the mean.

Just because an organization was able to complete a self-assessment questionnaire on PCI DSS compliance doesn't make them PCI DSS compliant. The results from the table clearly indicate that 20.6% strongly disagreed with that statement, whereas 55.9% disagreed with it.

Table 4.3.9 Distribution of Respondents by whether a Completed Self-assessment Questionnaire (SAQ) makes one PCI DSS Compliant

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	7	20.6	20.6	20.6
Disagree	19	55.9	55.9	76.5
Neutral	7	20.6	20.6	97.1
Agree	1	2.9	2.9	100.0
Total	34	100.0	100.0	

Mean =2.06, Standard deviation=0.74, n=34, Source: Research Data (2015)

4.4 Analysis on how Organizations have Implemented PCI DSS Compliance

Respondents were further asked to respond on a scale of 1-5 on the extent to which organizations have implemented PCI DSS.As earlier elucidated in this report, the approach for analysis would be to looking at *mean* and *standard deviation* as parameters for measuring the extent to which organizations have implemented PCI DSS. The variables that respondents were required to respond to were ‘Build and Maintains a Secure Network’, ‘Protects Cardholder Data’, ‘Maintains a Vulnerability Management Program’, ‘ Implemented Strong Access Control Measures’, ‘Regularly Monitors and Tests Networks’ and ‘Maintains an Information Security Policy’.

The table below describes the average ratings of respondents on their view on the analysis of their organizations have implemented PCI DSS. From the table, ‘protects card holder’ had the highest mean 4.46 while ‘maintains vulnerability management program’ had the lowest mean 3.76 their standard deviation are within accepted range of not more than 3 showing the data is well spread around the mean.

Table 4.4 Analysis of how Organizations have Implemented PCI DSS Compliance

Variable Name	N	Mean	Mode	Std. Deviation
Build and Maintains a Secure Network	34	4.18	5	.796
Protects cardholder data	34	4.46	5	.700
Maintains a vulnerability management program	34	3.76	4	1.045
Implemented Strong Access Control Measures	34	4.18	5	.904
Regularly Monitors and Tests Networks	34	3.85	4	1.077
Maintains an Information Security Policy	34	3.91	5	1.190

Source: Research Data (2015)

4.5 Analysis of Challenges Experienced in Implementing PCI DSS Compliance

The challenges of implementing PCI DSS compliance was measured by use of variables that required a respondent to rate their perception on challenges in implementing PCI DSS compliance on 10 variables by 'Strongly agreeing' 'Agree' Neutral' 'Disagree' 'Strongly disagree'. The tables will show description on how the respondents rated their perception on challenges of implementing PCI DSS compliance in their companies. To generate the *means* and *standard deviations* responses were coded and given numerical values as follows: *Strongly Agreed=5; Agreed=4; Neutral=3; Disagreed=2; Strongly Disagreed=1*.

4.5.1 Distribution of Respondents by whether PCI DSS Compliance is Effective

The table below describes the perception of respondents on a challenge of whether PCI DSS compliance is effective or not. The mean value of responses was 4.18 and a standard deviation of 0.76.The mean value showed that the responses tended more towards '*Agree*' and dispersion of responses from the mean was within tolerable limit i.e. the data is well spread around the mean.

From the results in the table, a large percentage of respondents, 64.7% agree that the PCI DSS is effective. The percentage of respondents that either disagreed or agreed was a paltry 5.4%.

Table 4.5.1 Distribution of Respondents by whether PCI DSS Compliance is Effective

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	1	2.9	2.9	2.9
Neutral	1	2.9	2.9	5.9
Agree	22	64.7	64.7	70.6
Strongly Agree	10	29.4	29.4	100.0
Total	34	100.0	100.0	

Mean =4.18, Standard deviation=0.76, n=34, Source: Research Data (2015)

4.5.2 Distribution of Respondents by whether PCI DSS is very Costly to Implement

The table below describes the perception of respondents on a challenge of whether PCI DSS is very costly to implement. From the table, commutatively a large percentage of respondents either agreed (50%) or strongly agreed (23.5%) that PCI DSS is very costly to implement. The percentage of respondents that disagreed was a paltry 2.9%. The mean value of responses was 3.94 and a standard deviation of 0.78.The mean value showed that the responses tended more towards '*Agree*' and dispersion of responses from the mean was within tolerable limit i.e. the data is well spread around the mean.

Additionally, it will be critical to note that there cannot be compliance without the involvement of costs, at least they need to be justified which in this case, the PCI DSS standard clearly advises what is required prior to the implementation.

Table 4.5.2 Distribution of Respondents by whether PCI DSS is very Costly to Implement

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Disagree	1	2.9	2.9	2.9
Neutral	8	23.5	23.5	26.5
Agree	17	50.0	50.0	76.5
Strongly Agree	8	23.5	23.5	100.0
Total	34	100.0	100.0	

Mean =3.94, Standard deviation=0.78, n=34, Source: Research Data (2015)

4.5.3 Distribution of Respondents by whether PCI DSS Certification is Difficult to Maintain

The table below describes the perception of respondents on a challenge of whether PCI DSS certification is difficult to maintain. From the table, the distribution of respondents were larger around Disagree (23.5%), Neutral (26.5) and Agree (35.3%). This was reflected also with mean value of 3.18 that showed that responses tended towards 'neutral' response. The standard deviation of 1.09 from the mean was within tolerable limit i.e. the data is well spread around the mean.

According to the study, 35.3% of the respondents felt that PCI DSS certification is difficult to maintain. This maybe partly due to operationalization of what the compliance dictates or the cost of compliance, and most times it is both, more so when PCI DSS is viewed as an annual exercise as opposed to it being a continuous effort of existence for a Payment Card Company.

Table 4.5.3. Distribution of Respondents by whether PCI DSS Certification is Difficult to Maintain

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	2	5.9	5.9	5.9
Disagree	8	23.5	23.5	29.4
Neutral	9	26.5	26.5	55.9
Agree	12	35.3	35.3	91.2
Strongly Agree	3	8.8	8.8	100.0
Total	34	100.0	100.0	

Mean =3.18 Standard deviation=1.09, n=34, Source: Research Data (2015)

4.5.4 Distribution of Respondents by whether Business Teams don't understand the Intricate Mechanics of Card Transactions

The table below describes the perception of respondents on a challenge of whether business teams don't understand the intricate mechanics of card transactions. From the table, there was no clear majority of respondents of either agreeing or disagreeing with the challenge. To that end, it was noted that 29.4% agree with the statement that the business teams do not understand the intricate mechanics of card transactions.

This was also reflected with mean value of 3.29 that showed that responses tended towards ‘neutral’ response. The standard deviation of 1.19 also showed that data was well spread around the mean.

Table 4.5.4 Distribution of Respondents by whether Business Teams don't understand the Intricate Mechanics of Card Transactions

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	2	5.9	5.9	5.9
Disagree	8	23.5	23.5	29.4
Neutral	8	23.5	23.5	52.9
Agree	10	29.4	29.4	82.4

Strongly Agree	6	17.6	17.6	100.0
Total	34	100.0	100.0	

Mean =3.29 Standard deviation=1.19, n=34; Source: Research Data (2015)

4.5.5 Distribution of Respondents by whether the Individual PCI DSS Requirements are overwhelmingly many

The table below describes the perception of respondents on a challenge of whether individual PCI DSS requirements are overwhelmingly many. From the table, the distribution of respondents were larger around Disagree (20.6%), Neutral (29.2) and Agree (41.2%). This was reflected also with mean value of 3.15 that showed that responses tended towards ‘neutral’ response. The standard deviation of 0.98 from the mean was within tolerable limit i.e. the data is well spread around the mean.

From the study, 41.2% agreed that the individual PCI DSS requirements are overwhelmingly many. This is understandably so mainly due to the inherent nature of data, it just has to be secured, and all systems handling data need to be foo proof hence the stringent requirements by PCI DSS compliance standard.

Table 4.5.5 Distribution of Respondents by whether the Individual PCI DSS Requirements are overwhelmingly many

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	2	5.9	5.9	5.9
Disagree	7	20.6	20.6	26.5
Neutral	10	29.4	29.4	55.9
Agree	14	41.2	41.2	97.1
Strongly Agree	1	2.9	2.9	100.0
Total	34	100.0	100.0	

Mean =3.15 Standard deviation=0.98, n=34, Source: Research Data (2015)

4.5.6 Distribution of Respondents by whether there is always the Lack of Management's Full Approval of Compliance Exercise

The table below describes the perception of respondents on a challenge of whether there is always the lack of management's full approval of compliance exercise. From the table, the distribution of respondents were larger around Disagree (23.5%), Neutral (29.5) and Agree (20.6%). This was reflected also with mean value of 2.97 that showed that responses tended towards ‘neutral’ response. The standard deviation of 1.29 from the mean was within tolerable limit i.e. the data is well spread around the mean.

From the study, the respondents were very much divided on this one. However, it is important to note that 20.6% agreed that there was always the lack of management’s full approval. Essentially, this means that without all the stakeholders’ approval, PCI DSS compliance will be next to impossible to achieve.

Table 4.5.6 Distribution of Respondents by whether there is always the Lack of Management's Full Approval of Compliance Exercise

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	5	14.7	14.7	14.7
Disagree	8	23.5	23.5	38.2
Neutral	9	26.5	26.5	64.7
Agree	7	20.6	20.6	85.3
Strongly Agree	5	14.7	14.7	100.0
Total	34	100.0	100.0	

Mean =2.97 Standard deviation=1.29, n=34, Source: Research Data (2015)

4.5.7 Distribution of Respondents by whether many Organizations have Legacy Systems thus making Compliance a Difficult Task

The table below describes the perception of respondents on a challenge of many organizations have legacy systems thus making compliance a difficult task. From the table, commutatively a large percentage of respondents either agreed (38.2%) or strongly agreed (20.6%) that many organizations have legacy systems thus making compliance a difficult task. But the mean value of responses was 3.94showed responses tended towards ‘neutral’.

Notably, there 38% of the respondents in the study who felt that the use of legacy systems make PCI DSS compliance a difficult task. This is because technology has evolved so much that components may not be compatible with each other when not fully updated to current versions. This goes to both software and hardware elements of a system. Therefore, upgrades are essential for a smooth transition towards a Payment Card Company becoming PCI DSS certified.

Table 4.5.7 Distribution of Respondents by whether many Organizations have Legacy Systems thus making Compliance a Difficult Task

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	3	8.8	8.8	8.8
Disagree	6	17.6	17.6	26.5
Neutral	5	14.7	14.7	41.2
Agree	13	38.2	38.2	79.4
Strongly Agree	7	20.6	20.6	100.0
Total	34	100.0	100.0	

Mean =2.97 Standard deviation=1.29, n=34, Source: Research Data (2015)

4.5.8 Distribution of Respondents by whether many IT Practitioners' Level of Comprehension to PCI DSS Compliance mostly has Gaps

The table below describes the perception of respondents on the challenge of many IT practitioners level of comprehension to PCI DSS compliance mostly have gaps. From the table, commutatively a large percentage of respondents either agreed (44.1%) or strongly agreed (20.6%) that of many IT practitioners level of comprehension to PCI DSS compliance mostly have gaps. But the mean value of responses was 3.71 showed responses tended towards 'agree'.

44% of the respondents in this study agreed with this challenge. This goes to show why there is a general feeling in the Payment Card Industry that PCI DSS compliance is difficult to implement. It is believed that when the workforce is enlightened about PCI DSS, could be either through training and/or workshops, this challenge may be eliminated.

Table 4.5.8 Distribution of Respondents by whether many IT Practitioners' Level of Comprehension to PCI DSS Compliance mostly has Gaps

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	1	2.9	2.9	2.9
Disagree	3	8.8	8.8	11.8
Neutral	8	23.5	23.5	35.3
Agree	15	44.1	44.1	79.4
Strongly Agree	7	20.6	20.6	100.0
Total	34	100.0	100.0	

Mean =3.71 Standard deviation=1.00, n=34, Source: Research Data (2015)

4.5.9 Distribution of Respondents by whether QSA Personnel are needed

The table below describes the perception of respondents on a challenge of whether QSA personnel are not needed. From the table, commutatively a large percentage of respondents either disagreed (50%) or strongly agreed (29.4%) that QSA personnel are not needed. The mean value of responses was 1.94 showed responses tended towards 'disagree'.

From the study, 50 % of the respondents agree that a QSA is necessary when an organization needs to get PCI DSS certified. The QSA is the person who will offer professional guidance with regards to the compliance. This person also makes the journey towards being compliant easier, and faster.

Table 4.5.9 Distribution of Respondents by whether QSA Personnel are needed

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly	10	29.4	29.4	29.4

Disagree				
Disagree	17	50	50	79.4
Neutral	6	17.6	17.6	97.1
Agree	1	2.9	2.9	100
Total	34	100	100	

Mean =1.94, Standard deviation=0.766, n=34, Source: Research Data (2015)

4.5.10 Distribution of Respondents by whether the Larger the Cardholder Environment, the more Difficult it is to fully meet PCI DSS Compliance

The table below describes the perception of respondents on a challenge of the larger the cardholder environment the more difficult it is to fully meet PCI DSS compliance. From the table, there was no clear majority of respondents of either agreeing or disagreeing with the challenge. This was reflected also with mean value of 3.06 that showed that responses tended towards 'neutral' response. The standard deviation of 1.23 also showed that data was well spread around the mean.

From this study, majority of the respondents 11.8% and 26.5% strongly disagree and agree, respectively, with the statement that the larger the cardholder environment ,the more difficult it is to fully meet PCI DSS compliance. This also depicts the fact that it doesn't matter the quantity of card data a Payment Card Company hosts, PCI DSS compliance is necessary for all Payment Card Companies.

Table 4.5.10 Distribution of Respondents by whether the Larger the Cardholder Environment, the more Difficult it is to fully meet PCI DSS Compliance

Type of Response	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	4	11.8	11.8	11.8
Disagree	9	26.5	26.5	38.2
Neutral	5	14.7	14.7	52.9
Agree	13	38.2	38.2	91.2
Strongly Agree	3	8.8	8.8	100.0
Total	34	100.0	100.0	

Mean =3.06, Standard deviation=1.23, n=34, Source: Research Data (2015)

4.6 Ranking of Challenges in Implementing PCI DSS Compliance

Respondents were further asked to respond on a scale of 1-5 on the challenges on implementing PCI DSS.As earlier elucidated in some sections of this report, the approached for analysis would be to look at *mean* and *standard deviation* as parameters for measuring for ranking challenges implementing PCI DSS.

From the table high cost implications (mean=4.26) was ranked as the biggest challenge in implementing PCI DSS compliance while PCI DSS being seen as an annual activity(mean =3.32) was ranked as least challenging. The standard deviations from the mean for all variables were within tolerable limits of 3 points implying the data was well spread around the means.

Table 4.6. Ranking of Challenges in Implementing PCI DSS Compliance

Variable Name(Challenge)	N	Mean	Std. Deviation	Rank
High Cost Implication	34	4.26	.790	1
Time consuming implementation	34	4.12	.913	2
Resource intensive	34	4.03	1.029	3
PCI DSS being seen as an annual activity	34	3.32	1.364	5
Lack of training	34	3.62	1.045	4

Source: Research Data (2015)

4.7 Regression Analysis of Security Concerns in Payment Card Companies

In this study, from the conceptual framework’s dependent variable (Security concerns) was measured by four variables namely Card skimming, Re-routing of transactions, Loss of business revenue and Penalties Levied; independent variables were educational level of respondents and PCI DSS compliance that was measured by nine variables as mentioned in preceding sections of this report. The data was transformed from categorical to numerical by assigning a numerical value to responses. Then linear regression was run using SPSS.

Model Summary

Table 4.7 Regression Analysis

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	454[a]	.206	.155	.51552

a. Predictors: (Constant), PCI COMPLIANCE, Level of Education of Respondent

b. Dependent Variable: SECURITY CONCERNS

Source: Research Data (2015)

R-Square - This is the proportion of variance in the dependent variable which can be explained by the independent variables). This is an overall measure of the strength of association and does not reflect the extent to which any particular independent variable is associated with the dependent variable. From the model summary output only 15.5 percent of the dependent variable (Security Concern) was explained by the PCI DSS compliance and level of education of respondents. The overall measure of association also looks weak as the R- squared is small value.

Coefficients

Table 4.7.1 Effects on Security Measures

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.064	.563		3.668	.001
Level of Education of Respondent	.499	.177	.463	2.823	.008
PCI DSS Compliance	-.054	.145	-.061	-.370	.714

Dependent Variable: Security Concerns, Source: Research Data (2015)

From the Table significance are larger (PCI DSS compliance= Sig.0.714) and lower for Level of Education of respondents (Sig=0.008) both than alpha 0.05 showing the variables education level had higher predictive power on Security concern and PCI DSS compliance had a lower predictive power on security concerns.

Level of education of the respondents had an influence on surmounting security concerns and that PCI DSS did not have a significant influence on addressing security concerns of card holder data. The level of education has a great impact on surmounting the card security concerns, and this is shown by t=2.823, which is greater than 1.96.This is because when one has been exposed to greater knowledge, they have the power to either be ethical and do good by securing card data or be unethical and commit fraud with the information they have access to. On the other hand, PCI DSS compliance did not prove, from the research, that it has significant power or influence, other than the fact that it is a global industry wide standard of governance for the payment card industry. Even with PCI DSS compliance, the level of education of the implementers needs to be of a higher degree of knowledge.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter will discuss the aim of the research, summary, recommendations and conclusions of the findings of the research. Limitations of the research and suggestions for further research have also been covered in this chapter.

5.2 Summary

This study was carried out to reveal the challenges that are experienced during the implementation of the PCI DSS standard, and how to surmount those23 challenges and maintain being PCI DSS certified.

From the study, it has been revealed that regardless of the size of the Payment Card Company, PCI DSS compliance is a necessity. It also doesn’t mean that PCI DSS is all inclusive as a security standard, and an emphasis should be made to ensure all security measures are put in place so safe guard cardholder data, whether it is stationary or in transmission. Additionally, it is not enough to just achieve compliance, it is very necessary to maintain it and this must be an ongoing exercise in the organisation as opposed to have it as an annual activity.

In as much as it is important for an organisation to maintain PCI DSS compliance, fraud may still happen. Unfortunately, this is because nothing can stop an errant employee from inappropriately handling cardholder data. For this reason. The study has revealed that some IT and Operations personnel do not have a clear understanding of their role in data security and PCI DSS compliance. This goes to reveal that awareness and training sessions are crucial for PCI DSS certification maintenance. This requires periodic training, and holding of employees, contractors and vendors responsible for their exposure to the chain of custody of PCI data. Moreover, for the aforementioned to be successful, all the stakeholders in the organisation need to fully, and positively support the PCI DSS endeavour.

Also, revealed from the study that a payment card organisation must know its infrastructure well so as to implement security controls effectively. From the study, it was also noted that Payment Card Companies need to also implement security programs, in addition to PCI DSS. It is for this reason that employing the services of a qualified security assessor (QSA) is important. This person's role will be to ensure the systems in the organisation are reasonably secure at all time. He is an ally to the organisation, and not a threat.

5.3 Conclusions

The PCI DSS standard has been in existence for nearly a decade, and it is here to stay. Card service providers from around the world have adopted it. That is, from merchants, service providers and Payment Card companies have adopted the compliance standard. PCI DSS is designed to standardize and assess how Payment Card companies are protecting the card data they hold from threats.

PCI DSS is not an end in itself as a security standard, nonetheless, it sure does reduce incidences in card data fraud. So it is globally accepted and acknowledged as the Payment Card Industry standard, but the questions that still lingers are; is it effective? Is it possible to achieve it? The research study suggests that the level of education of the respondents had an influence on surmounting security concerns and that PCI DSS did not have a significant influence on addressing security concerns of card holder data. The level of education has a great impact on surmounting the card security concerns. This is because when one has been exposed to greater knowledge, they have the power to either be ethical and do good by securing card data or be unethical and commit fraud with the information they have access to. On the other hand, PCI DSS compliance did not prove, from the research, that it has significant power or influence, other than the fact that it is a global industry wide standard of governance for the payment card industry. Even with PCI DSS compliance, the level of education of the implementers needs to be of a higher degree of knowledge.

5.4 Recommendations

The effort required for the implantation of PCI DSS should not be underestimated. PCI DSS compliance needs a lot of resources; money, time and executive buy-in and sponsorship. It requires an organisation wide attention where everyone is involved and are made aware of the role that they play in data security; system developers, system administrators, executives, customer service staff and not just the IT security team.

The organisation must make compliance sustainable. There are so many tasks that an organization must complete throughout the year to stay PCI DSS compliant. For this to be sustainable, compliance needs to be embedded in the daily operations of an organisation as an ongoing process.

When properly implemented, PCI DSS drive process improvements, generate additional revenue and cut costs, and identify opportunities to consolidate infrastructure. For instance, storing less data in fewer systems in the organisation can cut costs and free up back up resources for other critical organisational needs. The organisation should leverage PCI DSS compliance as an opportunity and not view it as burdensome.

Any Payment Card Company should have a strategy for compliance. The organisation should think of compliance in a wider context and incorporate it in their strategic placement. This makes it fairly easy for PCI DSS maintenance.

5.5 Limitations

The research was conducted successfully and the research objectives were met. However, there were some limitations. First, the time dedicated to the project was not enough due to work and school demands and deadlines, respectively. This made it hard to distribute and collect the questionnaires. Secondly, access to the information was not very easy as some respondents were not willing to complete the questionnaire since they were suspicious of the intentions of the study, and did not feel it was safe to share everything they knew.

5.6 Suggestions for future research

This research was designed to specifically look into how an organisation can surmount the challenges of complying with the Payment Card Industry data security standard (PCI DSS). It is recommend that further research on this be carried out in the East Africa region, because this research was done for only Kenya. This will provide a much broader perspective on the subject. Follow up research can also be done to enhance the body of knowledge.

REFERENCES

27001 Academy. (2014). Retrieved August Sunday 2/8/2015, 2015, from 27001 Academy: http://advisera.com/27001academy/knowledgebase/pci-dss-vs-iso-27001-part-2-implementation-and-certification/

Acunetix. (2015, June 19). Retrieved June Wednesday 17/6/2015, 2015, from http://www.acunetix.com: http://www.acunetix.com/websitesecurity/pci-compliance-wp/

Bendigo and Adelaide Bank. (2006). *A guide to implement the Payment Card Industry Data Security Standard (PCI DSS).*

Capra, F. (1997). *The web of life.* New York: Doubleday-Anchor Book.

Checkland, P. (1997). *Systems Thinking, Systems Practice.* Chichester: John Wiley & Sons Ltd.

Chiu, S. C. (2011). *Payment Card Industry Data Security Standard.* University of Waterloo: Research Paper.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, pp. 319-339.

Dimension Data. (2011). *Understanding the 12 Requirements of PCI DSS.* Opinion Piece.

E-Path. (2015, June 18). Retrieved May Saturday 23/5/2015, 2015, from https://e-path.com: https://e-path.com.au/pcidss.html

First Data Corporation. (2009, July). PCI DSS and Handling Sensitive Cardholder Data—Why You Care. Retrieved July Wednesday 1/7/2015, 2015

French, C. (1996). *Data Processing and Information Technology.* UK: Thompson.

Gartner. (2008, May 16). PCI Compliance Remains Challenging and Expensive.

Haag, S. C. (2002). *Management Information Systems for the Information Age*. Boston: McGrawHill.

Himma, K. E. (2007). *Internet Security;Hacking,Counterhacking and Society.* London: Jones and Bartlett.

IT Governance. (2003-2015). Retrieved August Sunday 2/8/2015, 2015, from IT Governance: http://www.itgovernance.co.uk/pci_dss.aspx

Jefwa, B. (2015, July Wednesday 15/07/2015). Retrieved July Monday 13/7/2015, 2015, from All Africa: http://allafrica.com/stories/201507132399.html

Kellert, S. (1993). *In the wake of Chaos:Unpredicable order in Dynamical Systems.* Chicago,USA: University of Chicago Press.

Kenswitch Ltd. (2014, June 10). Retrieved June Thursday 11/6/2015, 2015, from Kenswitch website: http://www.kenswitch.com/

Kenya Bureau of Standards. (2014). Retrieved August Thrusday 6/8/2015, 2015, from KEBS: http://www.kebs.org/index.php?opt=certification&view=isms

Kothari, C. (2004). *Research Methodology,Methods and Techniques.* New Delhi: New Age International Publishers.

Landon, K. C. (2007). *Essentials of Business Information Systems.* New Jersey: Prentice Hall.

MasterCard Worldwide. (2005). *All About Payment Cards.*

McAfee for Business. (2015, June 18). Retrieved June Tuesday 23/6/2015, 2015, from http://www.mcafee.com/: http://www.mcafee.com/us/services/strategic-consulting/compliance/payment-card-industry-pci-security-solutions.aspx#vt=vtab-KeyBenefits

Miller, N. W. (2015, February 4). The Target and Other Financial Data Breaches:Frequently Asked Questions. *Congressional Research Service*.

Omukhweso, W. A. (2012). *The Role of ISO Standards in Kenya's Economy*. Nairobi: Kenya Bureau of Standards.

O'neill, J. (2015, March 26). Retrieved June Monday 1/6/2015, 2015, from Netwrix Community: http://blog.netwrix.com/2015/03/26/pci-dss-v3-number-one-implementation-hurdle/

Paul De Hert, Y. P. (2010). *Data Protection in a Profiled World.* New York: Springer.

Paynet Ltd. (2014, November 10). Retrieved June Thursday 11/6/2015, 2015, from Paynet website: http://www.paynet.co.ke/

Paynet, N. (2014, November 7). Nairobi, Kenya. Retrieved June Tuesday 16/6/2015, 2015

PCI Security Standards Council. (2010, October). Payment Card Industry (PCI)Data Security Standard. *Requirements and Security Assessment Procedures*. Retrieved May Sunday 10/5/2015, 2015

PCI Security Standards Council. (2014, August). Best Practices for Maintaining PCI DSS Compliance. Retrieved July Tuesday 7/7/2015, 2015

Pennington, B. (2011, April). Retrieved June Monday 1/6/2015, 2015, from Brian Pennington: http://brianpennington.co.uk/2011/04/21/pci-dss-compliance-trends-study-2011/

Ponemon Institute. (2009, February). *2008 Annual Study:Cost of a Data Breach.*

Rouse, M. (2009, May 9). Retrieved May Friday 15/5/2015, 2015, from TechTarget: http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

Schmalensee, D. S. (2009). Innovation and Evolution of the payments Industry. *2009 Payments Brookings*, 36-75.

Techopedia. (2015, August 7). Retrieved May Sunday 24/5/2015, 2015, from Techopedia: http://www.techopedia.com/definition/26464/data-security

Tsoukas, H. (1998). Chaos, Complexity and Organization Theory. *Organization*, 291-313.

Verizon. (2009). *2009 Data Breach Investigations Report.* Verizon Business RISK Team.

Verizon. (2014). *Verizon 2014 Compliance Report.* Verizon. Retrieved August Tuesday 11/08/2015, 2015, from http://www.cisco.com/web/strategy/docs/retail/verizon_pci2014.pdf

Vijayan, J. (2014, Ferbruary 7). *Computer World.* Retrieved from http://www.computerworld.com: http://www.computerworld.com/article/2487457/malware-vulnerabilities/maintaining-pci-compliance-is-a-big-challenge-for-most-companies.html

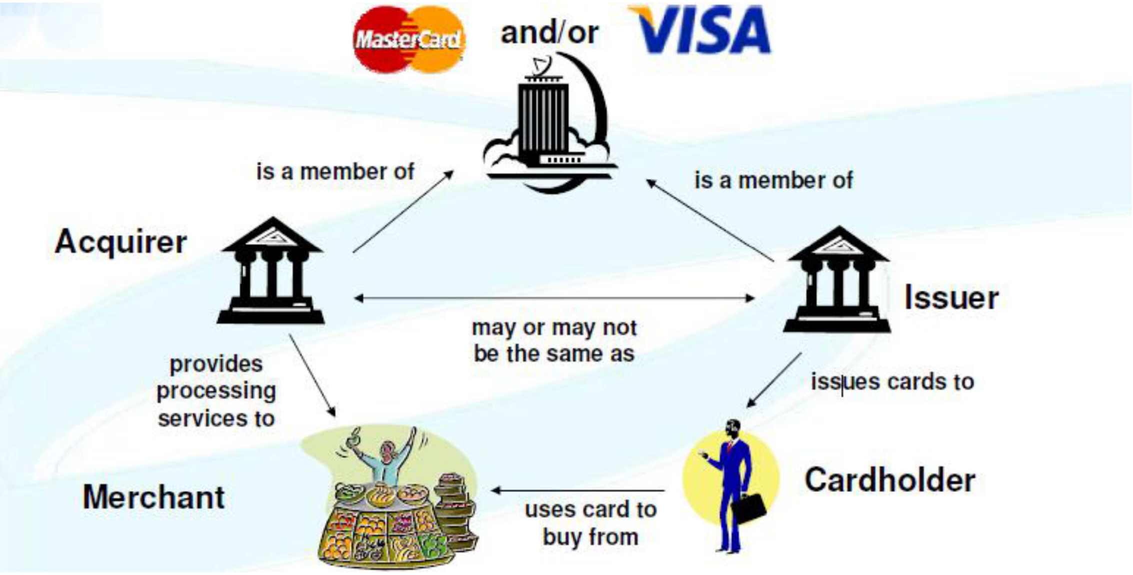
Westpac Banking Corporation. (2011, April 14). Retrieved May Saturday 9/5/2015, 2015, from Westpac Banking Corporation: https://www.westpac.com.au/docs/pdf/bb/Guide_to_payment_card_indus1.pdf

wikipedia. (2015, June 2). Nairobi, Kenya.

Xia, R. Y. (2011). *Insight to Payment Card Industry Data Security Standards (PCI DSS).* Research Paper, University of Waterloo.

APPENDICES

Appendix I: Related Parties within PCI DSS



Source: (Xia, 2011)

Appendix II: The Objectives and Requirements of PCI DSS

Below are the six objectives and twelve requirements for PCI DSS Compliance.

Build and Maintain a Secure Network

- **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data
- **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- **Requirement 3:** Protect stored cardholder data
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- **Requirement 5:** Use and regularly update anti-virus software
- **Requirement 6:** Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- **Requirement 7:** Restrict access to cardholder data by business need-to-know
- **Requirement 8:** Assign a unique ID to each person with computer access
- **Requirement 9:** Restrict physical access to cardholder data

Regularly Monitor and Test Networks

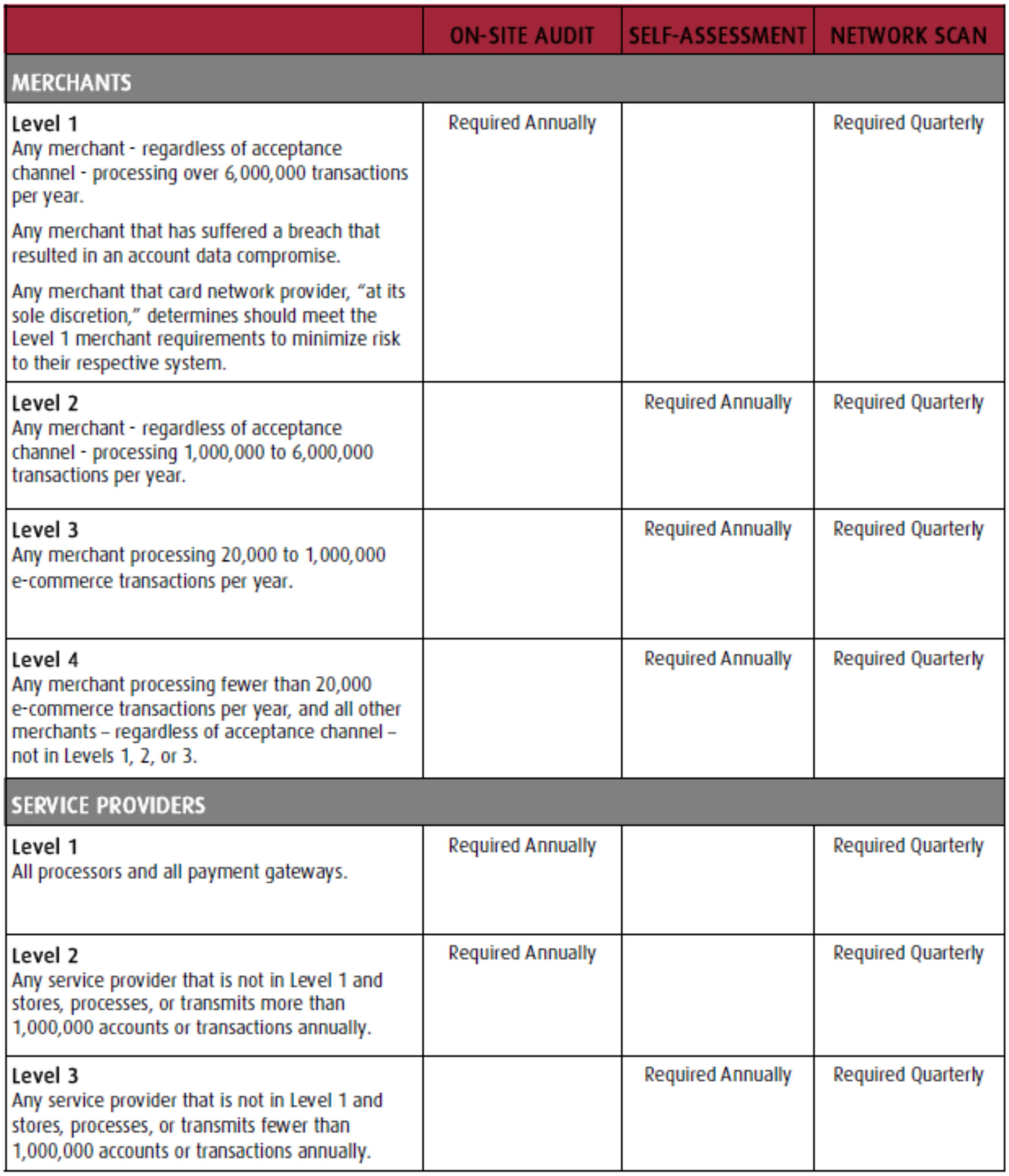
- **Requirement 10:** Track and monitor all access to network resources and cardholder data
- **Requirement 11:** Regularly test security systems and processes

Maintain an Information Security Policy

- **Requirement 12:** Maintain a policy that addresses information security

Source: "A Brief Description of the 12 PCI DSS Requirements” NDB Advisory. 5 June 2011.

Appendix III: Merchant and Service Provider Levels and Validation Requirements



	ON-SITE AUDIT	SELF-ASSESSMENT	NETWORK SCAN
MERCHANTS			
Level 1 Any merchant - regardless of acceptance channel - processing over 6,000,000 transactions per year. Any merchant that has suffered a breach that resulted in an account data compromise. Any merchant that card network provider, "at its sole discretion," determines should meet the Level 1 merchant requirements to minimize risk to their respective system.	Required Annually		Required Quarterly
Level 2 Any merchant - regardless of acceptance channel - processing 1,000,000 to 6,000,000 transactions per year.		Required Annually	Required Quarterly
Level 3 Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.		Required Annually	Required Quarterly
Level 4 Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants – regardless of acceptance channel – not in Levels 1, 2, or 3.		Required Annually	Required Quarterly
SERVICE PROVIDERS			
Level 1 All processors and all payment gateways.	Required Annually		Required Quarterly
Level 2 Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 accounts or transactions annually.	Required Annually		Required Quarterly
Level 3 Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 accounts or transactions annually.		Required Annually	Required Quarterly

Source: (Xia, 2011)

Appendix IV: Questionnaire

This questionnaire seeks to collect data on the extent to which the Payment Card companies in Kenya are PCI DSS compliant. Kindly note all information provided will be kept confidential and will be used for academic research purposes only. Please answer all questions.

Section A: General Demographics

1. What is your gender?

   Male □ Female □

2. What is the name of the company you work for? ___________________________________

3. Which department do you belong to? ____

4. What is your level of education?

   University Bachelor’s degree □ College Diploma □ College certificate □

5. Do you have additional IT related certificates?

   Yes □ No □

6. Do you know what PCI DSS standard is?

   Yes □ No □

7. Is your organization PCI DSS certified?

   Yes □ No □

8. How concerned are you about card related crimes?

   Extremely concerned □
   Very concerned □
   Neutral □
   Slightly concerned □
   Not concerned at all □

Please write additional comments below.

____

____

Section B: Extent of PCI DSS compliance

1. Please indicate the extent to which you agree or disagree with the following perception statements regarding PCI DSS compliance in organizations.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.PCI DSS is too hard					
2.PCI DSS is unreasonable and requires too much					
3.We don’t have a lot of card transactions to be compliant					
4.PCI DSS makes organizations store card data					
5.PCI DSS will make us secure					
6.PCI DSS compliance is an IT project					
7.One vendor can make an organization PCI DSS compliant					
8.Outsourcing card processing makes an organization PCI DSS compliant					
9.We completed a self-assessment questionnaire (SAQ), so we are PCI DSS compliant					

Please write additional comments below.

____

____

2. From the below questions, please indicate the extent to which your organization has implemented PCI DSS. Kindly tick only one box per question.

Key: The Likert scale has 5 as the highest score and 1 as the lowest score

	1	2	3	4	5
1. Build and Maintains a Secure Network					
2. Protects Cardholder Data					
3. Maintains a Vulnerability Management Program					
4. Implemented Strong Access Control Measures					
5. Regularly Monitors and Tests Networks					
6. Maintains an Information Security Policy					

Please write additional comments below.

Section C: Challenges in implementing PCI DSS compliance

1. Please indicate the extent to which you agree or disagree with the following statements regarding challenges in implementing PCI DSS compliance in organizations.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.PCI DSS compliance is effective					
2.PCI DSS is very costly to implement					
3.PCI DSS certification is difficult to maintain					
4.Business teams do not understand the intricate mechanics of card transactions					
5.The individual PCI DSS requirements are overwhelmingly many					
6.There is always the lack of					

Management’s full approval of the compliance exercise					
7.Many organisations have legacy systems thus making compliance a difficult task					
8.Many IT practitioners level of comprehension to PCI DSS compliance mostly has gaps					
9.QSA personnel are not needed					
10.The larger the cardholder environment, the more difficult it is to fully meet PCI DSS compliance					

Please write additional comments below.

____

____

2. How would you rank the following challenges in implementing PCI DSS compliance? Kindly tick only one box per question.

   Key: The Likert scale has 5 as the highest score and 1 as the lowest score

	1	2	3	4	5
1. High cost implications					
2. Time consuming implementation					
3. Resource intensive					
4.PCI DSS being seen as an annual activity					
5.Lack of training					
6.Use of legacy systems in the organisation to achieve compliance					

Please write additional comments below.

___

___

Section D: Security concerns in Payment Card Companies

Kindly tick only one answer per question.

1. How many card skimming incidents have you experienced in the last 6 months?

a) Between 1 and 50

b) Between 50 and 100

c) 100 and over

2. How many transaction routing incidents have you experienced in the last 6 months?

a) Between 1 and 50

b) Between 50 and 100

c) 100 and over

3. What is the value of the revenue lost in the last 6 months?

a) Between KES 100,000 and 500, 000

b) Between KES 100,000 and 500, 000

c) KES 1000,000 and over

4. What is the value of penalties levied against your company by institutions within the Payments Industry?

a) Between KES 100,000 and 500, 000

b) Between KES 100,000 and 500, 000

c) KES 1,000,000 and over

Please write additional comments below.

___

___