AN INVESTIGATION OF THE LEVEL OF SECURITY ON AUTOMATED TELLER MACHINES (ATM) IN ZAMBIA BASED ON PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

By

ELLA NSONTA KASANDA

A DISSERTATION SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF ENGINEERING DEGREE IN ICT SECURITY

THE UNIVERSITY OF ZAMBIA

LUSAKA

2019

COPYRIGHT

DECLARATION

I, **Ella Nsonta Kasanda** hereby declare that the work presented in this dissertation is my own, and that to the best of my knowledge, it has not been previously produced or submitted before for a degree, diploma or other qualification at this university or any other institution for academic purposes, and that all sources of information have been duly acknowledged.

Author:

Full Name: Ella Nsonta Kasanda

_____ _____

Signature Date:

Supervisor:

Full Name: Dr. Jackson Phiri

_____ _____

Signature Date:

APPROVAL

This dissertation of Ella Nsonta Kasanda is approved as fulfilling the partial requirements for the award of the degree of Master of Engineering in ICT Security by the University of Zambia.

Internal Examiner 1	**Signature**	**Date**
Internal Examiner 2	**Signature**	**Date**
Internal Examiner 3	**Signature**	**Date**
Chairperson – Board of Examiners	**Signature**	**Date**
Supervisor	**Signature**	**Date**

DEDICATION

This dissertation is dedicated to my husband Obed and my sons Nsofwa, Emmanuel and Lutanda for the support, understanding, and encouragement during this work. Thank you very much for everything.

ACKNOWLEDGEMENTS

I thank and praise the Almighty God for giving me knowledge, understanding and good health during the course of my study. I want to also thank all the lectures that taught me in this program, especially Dr. Jackson Phiri my supervisor, who gave me continuous support and encouragement. I also want to thank the Ministry of Higher Education for the financial support the offered me during my study.

ABSTRACT

Automated Teller Machines (ATM) have revolutionized banking in Zambia, as customers are able to conduct several banking activities without physical Interaction with bank staff. They have however brought with them challenges of cyber-crime. Banks in Zambia have suffered financial losses through ATM fraud. Compliance with the Payment Card Industry Data Security Standard (PCI DSS) can mitigate ATM cyber-crimes in Zambia. The objectives of this research are to investigate challenges and the level of security on ATMs in Zambia based on the PCI DSS standard, and to investigate the effect of the EMV chip and PIN card on ATM crime and finally propose a framework to address the challenges of ATM fraud in Zambia. To address the first objective, a baseline study was carried out using the twelve requirements of the PCI DSS framework. Purposive sampling was used to select Information Technology staff in charge of ATM security from eight commercial banks in Zambia and employees from two ATM vendor companies as the target population of the research. The statistical information from Bank of Zambia on the ATM frauds faced before and after the introduction of the EMV chip and PIN card was used to address the second objective. Based on the results from the first and second objectives a Framework was proposed to help reduce ATM fraud in Zambia. From the baseline study it has been established that all the eight participating banks are non-compliant to the PCI DSS Framework. The levels of compliance range from 50% to 83%. This compromises ATM security as a cyber-criminal only needs 1 non-compliance to compromise card holder data. The statistics from Bank of Zambia show that ATM fraud has continued to rise even after the introduction of the chip and PIN card. A 6 layered framework has been proposed to help banks enhance ATM security and to ensure the country is cyber-ready for emerging ATM crimes like Jackpotting. The PCI DSS is part of the security measures in the proposed framework.

Keywords*: Automated Teller Machine(ATM), Payment Card Industry Data Security Standard (PCI DSS), cybercrime, EMV chip and pin card, Software Whitelisting.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ACRONYMS

ANZ	Australia and New Zealand Banking Group
ATM	Automated Teller Machine
BSI	British Standards Institution
BOZ	Bank of Zambia
BWAC	BankWorld Automated Teller Machine Client
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information and Related Technologies
CRT	Cathode Ray Tube
CVC	Card Verification Code
CVV	Card Verification Value
DAD	Disclosure, Alteration, Destruction
EJ	Electronic Journal
EMV	Europay, Mastercard, Visa
GBNA	Global Bank Note Acceptor
GEIT	Governance Enterprise Information Technology
GPRS	General Packet Radio Service
GRC	Governance Risk and Compliance
GSM	Global Mobile Communication System
ID	Identification
ISMS	Information Security Management Standards
ITIL	Information Technology Infrastructure Library
LCD	Liquid Crystal Display
MAC	Money Access Card
NDC	National cash Register Direct Connect
NCR	National Cash Register

OBE	Officer of the Most Excellent Order of the British Empire
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
POS	Point of Sale
RBAC	Role Based Access Control
RCE	Remote Code Execution
RSA	Ron Rivest, Adi Shamir and Leonard Adleman
SQL	Structured Query Language
SSL	Secure Socket Layer
TTW	Through-the Wall
XFS	Extensions for financial services
XSS	Cross-Site Scripting
YDC	YT Direct Connect

CHAPTER ONE: BACKGROUND TO THE STUDY

1.1 Introduction

An automated teller machine (ATM) is a computerized telecommunications device that is used by financial institutions to offer various services to its customers [1]. It allows customers access to financial transactions such as cash withdrawals, cash deposits, money transfers and balance enquiries without the need for a bank employee and without accessing the banking hall. The invention of the ATM has proved to be an important technological development that has enabled financial institutions to provide services to their customers in a 24X7 environment. The ATM has improved the convenience of customers by giving them access to their cash wherever required from the nearest ATM. It provides convenience to ATM customers as they are able to perform their various transactions 24/7. Apart from the banking premises, ATMs are also placed in other locations like shopping malls, airports, grocery stores, filling stations, restaurants and many places where large numbers of people gather. In order for a transaction to be successful, the ATM machine has to communicate with the ATM switch which then communicates with the core banking system. Due to their importance in the banking industry and their increased use, ATMs need to be secured. The security objectives of communication in any network must satisfy confidentiality, integrity, availability, authentication, authorization, privacy, identification and accountability/ non-repudiation [2]. The main objectives of an ATM are confidentiality, data integrity, accountability, authentication, correct functionality, authorization, availability and access control [3]. A Personal Identification Number (PIN) or password is a very important aspect of the ATM security system and is a traditional way of authenticating and authorizing a user on an ATM [4]. A PIN thus ensures to secure and protect financial information of customers from unauthorized access.

ATMs contain large sums of money and are therefore a target for criminals. Cyber-crime on ATMs has been on the rise in the recent years and it doesn't only affect customers but also the banks [5]. In 2013, several commercial banks in Zambia were robbed of more than US$4 million, through a sophisticated cyber-crime syndicate by foreigners who were working with Zambians [6]. The cyber-criminals used ATM card skimming techniques to copy data from customer's magnetic stripe ATM cards which they reproduced and used them to steal the money. Commercial banks introduced the chip and PIN card as a counter measure to the ATM card skimming attack. The

banks have also been mandated to comply with the Payment Card Industry Data Security Standard (PCI DSS) to counter ATM fraud.

However, Cyber-criminals have come up with new ATM threats like ATM Card Shimming and ATM Jackpotting. ATM fraud is not only a problem in Zambia but is a global problem. In January 2018, a sum of US$1 million was stolen from ATMs in the United States of America through Jackpotting Attack [7].

1.2 Gap in Literature

From the various literature reviewed, it is noted that most researchers that have attempted to enhance ATM security by providing solutions to mitigate ATM risks all have dealt with risks associated with the authentication process on the ATM. These solutions have focused on the card skimming attack on the ATM, however new and emerging threats on the ATM like the Jackpotting attack cannot be mitigated by the use of security solutions like Biometric Authentication.

Most of the research has centered on the use of different biometric features to authenticate a cardholder on the ATM.

1.3 Scope

The research was conducted in Lusaka the capital city of Zambia. A baseline study was done on the level of ATM security in Zambia based on the PCI DSS. The research determined how compliant commercial banks in Zambia are, with the PCI DSS. This research also determined if the introduction of the EMV chip and PIN ATM cards has helped reduce ATM fraud in Zambia. The results of this research were used to propose a framework that will mitigate ATM crime in Zambia and help banks enhance ATM security. This Research covered ATM card fraud in relation to the ATM machine and ATM card fraud in relation to Point of Sale (POS) machine in Zambia. Online Transaction fraud is out of this research Scope.

1.4 Problem Statement

Crime in ATMs has become a global issue that faces not only customers, but also bank operators [8]. ATM frauds in Zambia and across the globe has increased in the recent years. Fraud techniques used by cyber-criminals have become more advanced. Managing the risk associated with ATM fraud, as well as diminishing its impact is an important issue that face financial institutions in

Zambia and the world at large. The traditional fraud technique that banks have been facing is ATM card skimming. With the coming of new ATM threats like Jackpotting, Banks in Zambia have a task of ensuring that they are cyber ready for these new threats.

1.5 Aim

To investigate the levels of ATM security based on the PCI-DSS standard and design a conceptual framework to enhance ATM security in Zambia.

1.6 Objectives

The specific objectives of this research are as follows:

(i) To investigate the level of security on ATMs in Zambia based on PCI DSS,

(ii) To determine if the introduction of chip and PIN card in Zambia has reduced ATM crime,

(iii)To propose a conceptual framework that will enhance ATM security in Zambia.

1.7 Research Questions

ATM fraud is a problem that commercial banks and its customers have continued to face. Research questions that this study required to answer were:

(i) What is the level of security on ATMs in Zambia based on PCI DSS?

(ii) Has the introduction of chip and PIN ATM card helped reduce ATM frauds in Zambia?

(iii) What framework can be used to enhance ATM security in Zambia?

1.8 Significance of the Study

This research will determine the level of ATM security in Zambia based on PCI DSS. It will also determine if the introduction of the EMV chip and PIN card in Zambia has helped to mitigate ATM fraud. A framework that will help Zambian commercial banks enhance ATM security will be proposed. The framework will secure ATM cardholder data. Safe ATMs will make customers gain more confidence in using the ATM and will improve the customers experience whilst using ATMs.

The findings of this research were published in International Journal of Advanced Studies in Computer Science & Engineering[1]

1.9 Organization of the Dissertation

The work done in this thesis is organised in 5 chapters.

Chapter 1 is the introduction of the thesis. It gives a brief overview and the background of the thesis. This chapter briefly describes the ATM, ATM fraud and PCI DSS framework. It gives the motivation and significance of this study. It also gives the scope of the research and states the problem of the research. It gives the aim and objectives of the thesis. It then lists the research questions that should be answered in order to achieve the objectives of the thesis. It gives the research contributions and then the chapter summary.

Chapter 2 is the background theory and related works. It reviews literature by other researchers and compares and contrasts the different literature. Chapter two also reviews works related to this research that have been done by other researchers.

Chapter 3 discusses the Methodology. It states the reasons for choosing the methodology used. It discusses the approach for the research, the sampling process and justification for considering data collection methods and instruments.

Chapter 4 gives the Results obtained from the data collection. It gives the actual results from the questionnaires and interviews. This was aimed at achieving the objectives.

Chapter 5 discusses the results obtained from the data collection. It discusses the results in relation to the body of knowledge on the subject being researched. It concludes and proposes a framework that can be adopted to enhance ATM security in Zambia.

[1] Kasanda, E. N., & Phiri, J. (2018). ATM Threats: A Case Study of Emerging Threats. International Journal of Advanced Studies in Computer Science and Engineering, 1-7.

1.10 Chapter Summary

This chapter looked at the introduction of this thesis. It began by discussing the ATM and its convenience in the financial institutions. It then stated the motivation, the gap in literature, significance and scope of this study. It stated the problem and then outlined the aim, objectives, research questions and contribution of this research. It concluded by outlining the organization of this thesis.

CHAPTER TWO: LITERATURE REVIEW

2.1 Chapter Introduction

This chapter reviews literature that relates to ATM fraud and ATM security. Literature review is necessary in order to find out what is already known on the subject matter [9]. The literature review helps the researcher to engage with published work so that they can show how their own study could add something to the body of knowledge. It also provides a context and a conceptual/ theoretical framework for the researcher's research and most importantly it shows how the investigation relates to, and builds on, previous research. The chapter reviews ATM risks. It is important to understand the risks associated with the ATM in order to know how to mitigate them as it is difficult to fight against something you do not understand.

The chapter also reviews literature that relates to PCI DSS as this is the standard used to carry out the baseline study in this research. The PCI DSS was selected for this research as Bank of Zambia (BOZ) which is the central bank in Zambia has mandated all commercial banks in the country to be compliant with the standard. Literature to see how PCI DSS relates to other international information security standards like Control Objectives for Information and Related Technologies (COBIT), ISO 27001, ITIL is also reviewed. Works that other researchers have done on PCI DSS is also reviewed to gain knowledge on how widely PCI DSS is used.

Literature on other security solutions that Researchers have recommended to help enhance the security of ATMs will also be reviewed. The framework 'Protect Mission Critical Assets' that has been adopted in this research is also discussed.

2.2 Review of the Literature

An ATM is a computerised telecommunications device used by bank customers to withdraw and deposit cash, get mini statements, get receipts, deposit cheques and make bill payments without entering the banking hall [1]. An ATM user is identified by using an ATM card and a PIN. The first ATM was installed in June 1967, by Barclays Bank in Enfield, north London [10].

2.2.1 Evolution of the ATM

The history of the ATM is full of interesting facts, some of which are known and others are unknown. According to the website www.engineersgarage.com/invention-stories/atm-history

[11], it is believed that the story of the ATM began when an Armenian named Luther George Simjian moved to the United States in 1920 under the account of Armenian Genocide. He had previously invented a portrait camera and then came up with the idea of ATM. He convinced himself of his invention and also convinced Citibank to use his product on trial for six months. Soon he was disappointed with the performance and lack of users and concluded that ATMs added no value to personal banking. The lack of ATM demand forced him to take a back seat and he clearly lost success and fame, and the same was passed on to two other gentlemen, John Shepherd-Barron and Don Wetzel.

John Shepherd-Barron was a Scottish national born in India who later moved to the UK and continued his studies at Edinburgh University and at Trinity College, Cambridge. After Shepherd-Barron returned empty-handed from a bank, he was disappointed that he had no choice but to wait for the bank to open its doors the next business day. He thought of a self-sufficient ATM which was invented in the early 1960s. The invention of a self-sufficient ATM was his second successful invention attempt. The internationally recognized four-digit standard PIN code was also invented by him. Previously, he had a six-digit serial number of the army in mind, but his wife then suggested a shorter PIN, as this would be easy to remember. Finally, in 1967, the first 24-hour ATM was commissioned. The ATM was installed in front of a Barclays bank branch in North London.

Today, ATMs are established around the world, giving everyone better access to their money, worldwide. Around 1.8 million ATMs are in operation worldwide, including cruise ships and navies, airports, news-stands and petrol stations. The developments have not stopped; Contactless technology is now booming. The same web site concludes that even at an advanced age, Shepherd-Barron had an inimitable and vivid interest in technology, foreseeing a future in which plastic cards would be numbered. In 2005, Shepherd-Barron received the OBE Award for his outstanding and memorable contributions to financial technologies. In 2010 he took his last breath and left his technological heritage.

2.2.2 The CIA Traid

The three fundamental principles of information security are confidentiality, integrity and availability as shown in Figure 1. All the controls and safeguards of information security and all of the threats, vulnerabilities, and security processes are bound by the C.I.A Traid.

Figure 1:CIA Traid [12]

An ATM like any other communications device should provide the information security requirements:

(i) Confidentiality: The first principle of the CIA Traid is confidentiality. It is the protection of data in storage and transit from unauthorized access, use, or disclosure [12]. Different security controls are required for the different states of data. The concept of confidentiality seeks to prevent unauthorized, intentional or otherwise disclosure of the content of a message. The loss of confidentiality can occur in a variety of ways, including intentional disclosure of information from private companies or incorrect application of network access rights.

(ii) Integrity: Integrity is the second principle of CIA Traid. Integrity is the assurance that the data has not been tampered with by unauthorized persons. This principle can be considered from three angles:

a) prevent changes by unauthorized persons,
b) prevent unauthorized changes by unauthorized persons,
c) maintaining the internal and external consistency of objects to ensure that their data is accurate and truly reflects the real world.

To maintain the integrity of a system, there must be controls that restrict access to data, objects, and resources. Multiple events can lead to integrity issues; accidentally deleting files, entering invalid data, changing the configuration, introducing a virus and running malicious code such as a Trojan. Integrity depends largely on confidentiality; without which it cannot be sustained.

(iii) Availability: In Information Security, the availability concept ensures fast and reliable access to data or IT resources by the right people. Availability thus ensures that the systems are ready for use when needed. In addition, this concept ensures the proper functioning of the security services required by the security expert. It should be noted that D.A.D. is the reverse of C.I.A. The opposite of confidentiality, integrity and availability is disclosure, alteration, and destruction (D.A.D.).

There are also other important information security concepts that the ATM should satisfy to protect card holder data. These concepts include identification, authentication, Accountability, authorization and privacy [12].

(iv) Identification: It is the means by which users assert their identity to a system. It is most commonly used for access control and is required for authentication and authorization.

(v) Authorisation: These are rights and permissions granted to a person (or process) to access an IT resource. Once the identity and authentication of the user are determined, the privilege levels determine the amount of system privileges that can be held by an operator.

(vi) Accountability /Non-Repudiation: Accountability is the ability to trace an action performed on a system to a user, a process or and application. Auditing, monitoring and logging are some of the actions that provide accountability.

(vii) Privacy: It is the privacy level and privacy protection granted to a user in a system. This is often an important part of the safety checks. Confidentiality not only guarantees the fundamental principle of the confidentiality of a company's data, but also the privacy of the data used by the operator.

(viii) Authentication: It is the process of identifying a person or system with the username and password. Authentication helps individuals and systems gain authorization based on their identify [13]. Authentication is achieved by combining one or more factors of a subject against a database of valid identities, such as user accounts.

2.2.2.1 Factors of Authentication

There are three basic types of authentication also known as three factors of authentication [14] as shown in Figure 2.

Figure 2: Authentication Factors [12]

A user can be authenticated on a system using one or two of the following authentication factors:

Type 1 Something you know: Examples include person identification number (PIN), password or passphrase.

Type 2 Something you have: These are physical things that a user possesses and can use to be authenticated. Examples are smartcard, hardware token, memory card and RSA ID. A memory card differs from a smartcard in that a memory card only stores information while a smartcard can process data. A smart card has a microprocessor and a certificate that can be used for authentication, to digitally sign and for encryption. A memory card only has authentication information for a user.

Type 3 Something you are: This is the use of physical biometric characteristics of a human being to be authenticated. Examples are fingerprint, hand geometry, iris pattern, retina pattern and face recognition.

The three types of authentication increase in strength if correctly implemented with type 1 being the weakest and type 3 being the strongest. However, attackers can still bypass type 3 authentication factors [14]. Cyber-criminals are able to fool a fingerprint reader by duplicating a fingerprint on a gummi bear candy.

Systems based on these types of authentication factors have the following limitations [15]:
1) access is typically bound to a single authentication occurrence leading to remote vulnerabilities,
2) the factors have little impact against persistent insider threats,
3) many of the authentication systems violate system design principles such as user psychological acceptability by inconveniencing the end-users.

Another factor different from the three basic types of authentication types known as Somewhere you are can be used [14]. It identifies the location of a subject based on a specific computer, a geographic location identified by an IP address or a phone number identified by caller ID. This factor is not effective when used on its own unless used in combination with the other three authentication factors.

In order to mitigate the identified limitations in the three basic methods of authentication, [15] proposed the usage of "where you are" as a complementary factor that can significantly improve both cybersecurity and physical security.

Using accurate location tracking as another factor for authentication:
1) Provides continuous identification tracking and continuous mediation of access to resources,
2) Requires remote threats to acquire a physical presence,
3) Allows for the enforcement of cybersecurity and physical security policies in real-time through automation,
4) Provides enhanced security without inconveniencing the end-users.

Requirements for an insider threat prevention system that is capable of actively monitoring malicious insider behaviors is incorporating somewhere you are factor in the other three basic types of authentication.

2.2.2.2 Multifactor Authentication

Multifactor authentication is an authentication that uses two or more factors. It can be implemented on the ATM to help mitigate ATM fraud by combing the PIN and biometrics. Two-factor

authentication requires two different factors for authentication. For example, if you use a debit card in the grocery store, you usually need to swipe your card (something you have) and enter a PIN (something you know) to complete the transaction. Similarly, smart cards typically require users to insert their card into a reader and enter a PIN. In general, using multiple types or factors will result in more secure authentication.

If two authentication methods of the same factor are used together, the strength of authentication is not greater than one method, since the same attack that could steal or get the first factor, could get the other as well. For example, using two passwords at the same time is not more secure than using a single passphrase, as an attempt to hack the password could detect both in a single successful attack. If two or more different factors are used, two or more different attack methods must successfully collect all relevant authentication elements. For example, if a token, password, and biometric factor are used for authentication, a physical robbery, password crack, and biometric duplication attack must be successful at the same time to allow an intruder to invade the computer System.

2.2.3 Automated Teller Machine Design

The design of an ATM is divided into physical and logical design.

2.2.3.1 Physical Design

The ATM is composed of the following input parts:

(i) Card Reader: The card reader captures the account information stored on the chip or magnetic stripe on the back of an ATM debit or credit card. The card reader is one of the most targeted devices on the ATM by cyber-criminals for ATM skimming attacks.

(ii) Keyboard: The keyboard is used by the cardholder to tell the ATM what kind of transaction is required (cash withdrawal, balance enquiry, cash transform, mini statement, Cash deposit, bills payment) and the cardholder also uses it to enter the PIN. The keyboard is another target of ATM card skimmers; they capture the PIN as a cardholder enters it.

The output components of the ATM are as follows:

(i) Display Screen: The display screen prompts the cardholder through each step of the transaction process. The two types of screen on an ATM is cathode ray tube (CRT) and LCD Screens.

(ii) Receipt Printer: The receipt printer provides the cardholder with a paper receipt of the transaction.

(iii) Cash Dispenser: The cash dispenser stores the money in the ATM and dispenses the money to the customer during a transaction. It is located in the bottom safe of the ATM. The cash dispenser uses either suction or friction to pick money from the cash canisters and present it to the customers. It has sensors throughout the carriage path that detects if there is money jammed.

Other ATM Devices are as follows:

(i) Cash Depository: There are two types of depositories on an ATM. The older version (4^{th} generation) of the ATM has a depository that uses envelops. A customer requests for an envelope and puts money in the envelop and then deposits the envelop into the ATM. The card holder's account is not credited immediately with the deposited amount until the ATM custodians go and physically count the money and then confirm the transaction. The second type of depository which is usually found on the newer version of the ATM (selfserv) is the Global Bank Note Acceptor (GBNA). The ATMs with this type of depository are called intelligent ATMs. This is because the GBNA is able to count the deposited money and credit the card holders account instantly. The GBNA is also able to determine if the money deposited is counterfeit money. It will take the money to the counterfeit bin but will not credit the cardholders account. If configured to, the GBNA has the ability to dispense the money that has been deposited. The intelligent ATMs are therefore sometimes known as recycling machines.

(ii) Journal Printer: The Journal printer prints a detailed record of all ATM activities including significant hardware and software events. It is a necessary component of any successful ATM network management strategy and is critical to the rapid resolution of hardware, software, security, or transaction issues threatening financial loss, device availability or customer relationships. An electronic Journal can be configured on an ATM in place of the physical journal printer. By managing the ATM's electronic journal (EJ) history and log remotely, banks save countless hours formerly spent maintaining journal receipts locally at the machine.

(iii)PC Core: This is the central processing unit for the ATM on which all the ATM software is installed. It has the same components like a personal computer i.e hard disk, mother board, processor and power supply. All the hardware components on the ATM connect to the PC core in order to work properly.

2.2.3.2 Logical ATM Software Design

Figure 3 shows the logical design of an ATM's software. The PC core of an ATM is first installed with an operating system like windows XP and windows 7. Aptra XFS is then installed on the PC to enable the PC communicate with the different physical devices of the ATM like card reader, cash dispenser, receipt printer, journal printer, encrypting pin pad and cash depository for the ATM models that are capable of accepting cash deposits. The application that customers will interact with as they are using the ATM is then installed on top of Aptra XFS. Different ATM software vendors call this application different names like Aptra NDC, Aptra YDC and BWAC. This is the application that also speaks to the ATM switch.

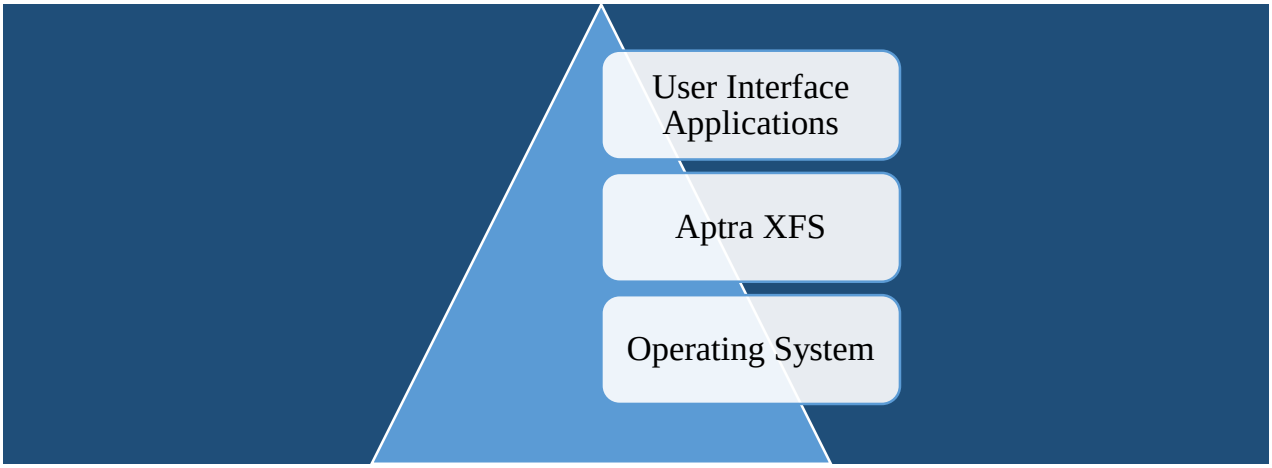

Figure 3: ATM Logical Design [16]

2.2.4 ATM Card Types

An ATM card is a payment card or a dedicated credit card issued by a financial institution that allows a customer to access ATMs. ATM cards are payment cards with magnetic stripe or plastic chip cards with a chip containing a unique card number and security information such as an expiration date and a card verification code (CVC) / Card Verification Value (CVV) [17] as is shown in Figure 4 and Figure 5.

A CVV / CVC on a credit or debit card is a three or four-digit number. A credit or debit card marked Visa or MasterCard has a three-digit number on the back of the card. On an American Express card, there are four-digit CVV values on the front of the card. CVV is an anti-fraud measure used to purchase a product without the need to enter a PIN or sign a receipt. The CVV number is required for online or telephone purchases. In this way, the merchant or the beneficiary can check if a person is actually the card holder and prevent people from using another person's card to perform fraudulent transactions.

An ATM card must always be stored safely as the CVV / CVC number is only printed on the card. If a card is lost or stolen, anyone can use it to make purchases online or over the phone without the owner's consent. The CVV / CVC number is called Secure Socket Layer (SSL) of an ATM card. This is a commonly used technology that is a digitally supplied certification process.

ATM cards are known by different names, such as Bank cards, Money Access Cards (MACs), loyalty cards, key cards or debit cards. Most payment cards, for example, debit and credit cards can also be used as ATM cards. Interbank networks permit the use of ATM cards by private operators and financial institutions other than the one issuing them.

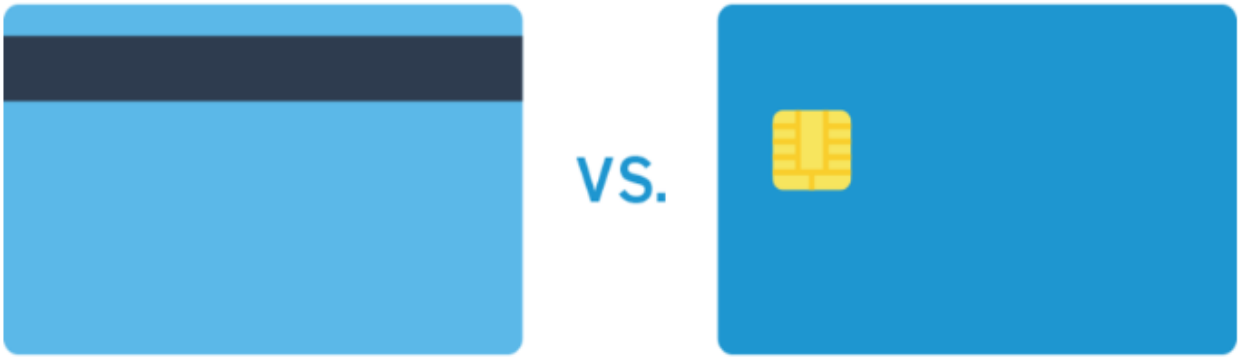

Figure 4: Magnetic Chip Card versus Chip and Pin Card [18]

Figure 5: Card Verification Code Versus Card Verification Value [18]

2.2.4.1 Differences between Magnetic Stripe Card and Chip and PIN Card

The security of smart cards is the latest standard in the security of credit cards. This standard (EMV®, developed and maintained by American Express, Discover, JCB, MasterCard, UnionPay and Visa) contains a small chip in the credit card that protects buyers from fraudulent transactions. Due to the changed credit card security, banks are eliminating magnetic stripe cards in favor of these safer, authenticated means of payment. But what exactly is the problem with magnetic stripe cards? And why are smart cards better?

First of all, magnetic stripe cards are quite outdated and have existed since the 1960s and use the same technology as cassettes. Surprisingly, the United States is one of the last countries to hold more of magnetic stripe cards. EMV has been the norm in most parts of the world for over a decade especially in European countries.

The main security features that help smart/chip cards combat fraud are:

(i) **EMV should prevent fraud**: EMV cards are primarily intended to prevent fraudulent transactions when a person physically places a counterfeit card on a payment terminal. In countries that have adopted EMV as a standard, some types of credit card fraud have dropped significantly.

(ii) **Chip cards are really hard to clone**: Magnetic stripe cards are well magnetized. When it is dragged, the payment processor reads its magnetic fields and compares them to the bank account information. The problem is that the data is static, which makes it easier for scammers to retrieve information and clone it on a new card. In fact, there is something called a skimmer which only costs US$ 20. On the other hand, the data on chip cards are

constantly changing, making the isolation and extraction of information extremely difficult. To decrypt it, someone should enter the physical circuit of the chip and manipulate the data to get the bank details. Not only is this level of data operation really difficult, it also requires a number of high-tech devices that can cost a million dollars. This is not the kind of money an average hacker has.

2.2.5 ATM Risk Management

Risk management seeks to reduce or eliminate vulnerabilities or reduce the impact of potential threats through the implementation of controls or countermeasures. It is neither possible nor desirable to eliminate the risks. Instead, an organization focuses on reducing the risks that are most damaging to their organization.

Key steps in a risk management process are as follows:

I. Identifying assets,
II. Identifying threats,
III. Identifying vulnerabilities.

A vulnerability is a weakness which can be due to a flaw or limitation in hardware or software, or the absence of a security control such as the absence of antivirus software on a computer [12]. A threat refers to a potential occurrence that can do harm to a system or your overall organization [12]. Risk refers to the likelihood or possibility that a threat will exploit a vulnerability and cause harm to an asset as indicated in equation 1 [12]:

$$\textit{Risk} = \textit{Threat} \times \textit{Vulnerability} \qquad \textit{Equation 1}$$

An ATM becomes vulnerable when there is a weakness in its security features. ATM security can be divided broadly into four categories namely: Physical Security, Software Security, Logical Security and Communication Security. ATM threats/attacks can be divided into physical and logical attacks. Physical attacks involve attacking the ATM physically like exploding the ATM safe to have access to the ATM safe money. In physical attacks, cyber-criminals use methods such as solid and gas explosives, as well as uprooting the ATM from the site and then using other methods to gain access to the safe. Other physical attacks involve placing of gargets on the ATM by cyber-criminals that copy ATM cardholder data and reproduce it on another card that can be

used to withdraw money from the cardholders' account. Logical attacks involve using malware to instruct the ATM to dispense money. This attack can be achieved by either gaining physical access on the ATM in order to install this malware on the ATM's PC Core or the malware can be injected through the network.

2.2.6 ATM Software Risks

NCR [16] categorises risks on the ATM software environment into 4 groups as can be seen in Figure 6.

2.2.6.1 Traditional Threats

Traditional Threats have been around for several years now. Traditional threats are things like viruses, worms and Trojans. Viruses are fairly easy to manage although occasionally cause a big impact on computer systems worldwide. A standard security software such as antivirus can be used to detect a well-known or less sophisticated attack that has taken place on a system [16].

Figure 6: ATM Threats [Source: NCR University]

Virus: A computer virus is a type of malicious program or code written to change the way a computer operates and is designed to spread from one computer to another [19]. It is the earliest form of malicious code security administrators had to deal with [20]. It operates by inserting or attaching itself to a genuine program or document that supports macros in order to execute its code. Most computer viruses are designed to affect or disrupt activities of the world's most popular

operating system Microsoft windows [20]. Antivirus software can be used to detect and eradicate the virus. Some of the most common types of antivirus software are Microsoft security essentials, Microsoft security defender, McAfee, Norton, Kaspersky and Symantec. Most anti-virus utilize a method called signature-based detection to identify potential virus infections on a computer system. An anti-virus keeps a database that contains known characteristics of all known viruses. Another method used by many anti-viruses is called heuristic-based mechanism to detect malware. In this method the anti-virus analyses the behavior of software looking for signs of viruses like attempts to elevate privilege level, cover their electronic tracks and alter unrelated or operating system files [20].

Worms: Worms are programs that replicate themselves from system to system without the use of a host file and pose significant risk to network security [20]. The first major incident in computer security was the internet worm. After that, hundreds of new worms have been unleashed like the code red worm and stuxnet. System administrators must ensure appropriate security patches are applied to their internet connected systems as soon as software owners release the patches.

Trojans: A Trojan is a type of malware which is a harmful software but looks legitimate. A Trojan carries a hidden payload that has the potential to cause havoc on a computer network [20]. Computer users should not download and install software from the internet unless they are absolutely sure they come from a trusted source. Untrusted software sources can bring Trojans onto computers and computer networks. Trojans differ in their operation as some will destroy all data stored on a network or system in order to cause damage in a short time frame. Some are harmless but will just install a value into windows registry that will cause a web page to open each time a computer is booted. The creators of such Trojans hope to gain money on adverts by the large number of page views they receive.

2.2.6.2 The Emerging Threats

These threats are stealthier, unusual, highly developed attacks which are more challenging to prevent using traditional security measures like anti-virus. This includes zero-day attacks, buffer overflows, code injection and application exploits. This category is a major risk to the security of ATMs as malware authors are becoming more sophisticated and criminalised.

Zero Day Attacks: A zero day exploit is a cyber-attack on a system exploiting a vulnerability that is unknown to others [21] [12]. This term may be used by security professionals in the following context; an attacker discovers a vulnerability first: An attacker can easily exploit a vulnerability when he is the one who discovers it before the software owners. The software vendor is not aware of the vulnerability and has not released a patch for the vulnerability.

Buffer overflows: Buffer overflows have been the most common form of security vulnerability for decades now [22] [23]. Buffer overflow vulnerability occurs when a user input is not properly validated by a developer to ensure that it is an appropriate size [20]. Remote network penetration vulnerabilities are dominated by buffer overflow vulnerabilities where an unidentified internet user seeks to gain control of a host. A significant portion of the most serious security threats would be eliminated if buffer overflow vulnerabilities are eliminated. In order to mitigate this risk [24]:

i. Buffer overflows should be identified during testing by entering increasingly larger values into form inputs, header and cookie fields,
ii. Unauthenticated sources should be prevented from inserting code,
iii. Input field length should be validated.

Code Injection: Code Injection, sometimes known as Remote Code Execution (RCE) refers to an attack where an attacker is able to execute malicious code as a result of an injection attack [25]. Code-injection attacks can occur at many layers; from the code to databases and web applications [26]. It is traditionally considered as a major threat and has been responsible for a large number of security breaches in past years [27]. A cyber-criminal can compromise a database using an SQL injection attack or the web browser's environment using a Cross-Site Scripting (XSS) attack.

2.2.6.3 Internal Threats

These are also tricky to detect and prevent. This covers a couple of scenarios; not just malicious insiders who install harmful applications, but also well-meaning employees who accidentally modify applications or install harmful software unintentionally. This might be unauthorised changes being rolled out at the wrong time, or untested patches being deployed which might bring the ATM down.

Business Risks: This represents the biggest new challenge for IT organisations globally. As a result of the Enron scandal in the US, under sections of the SARBANES OXLEY legislation any

company doing business with the US is having to spend millions of dollars on regulatory compliance [16]. This hasn't got as far as the ATM yet but it is heading that way.

PCI which is the Payment Card Industry Association (VISA and MasterCard), is bringing in similar IT regulatory requirements for ATMs. Many Banking organizations such as Interac in Canada and Carte Bancaire in France will be introducing similar requirements. Failure to comply with these requirements can result in huge costs for the Financial Institution.

2.2.7 ATM Threats

2.2.7.1 ATM Card Skimming Attack

ATM card skimming attack is a physical threat which has been the number one ATM threat globally in the past decade. ATM skimming refers to the stealing of the electronic card data, aiding the criminal to counterfeit the card. A skimmer is a device that is installed on a card reader making a customer believe they are inserting their card in the ATM card reader. The skimmer reads the data from a card's magnetic stripe or EMV chip when a client inserts it into the ATM. Some skimmers have the capability to read data from an EMV card chip at a distance. ATM skimming attacks are however on the decrease due to deployment of anti-skimming solutions, PCI DSS, EMV technology and contactless ATM functionality. Customers are unable to notice a problem and experience a normal ATM transaction until their account is defrauded. The most common places where skimmers are placed on the ATM are shown in Figure 7. Multifactor authentication using biometrics can be used as an added security mechanism against this type of fraud [4].

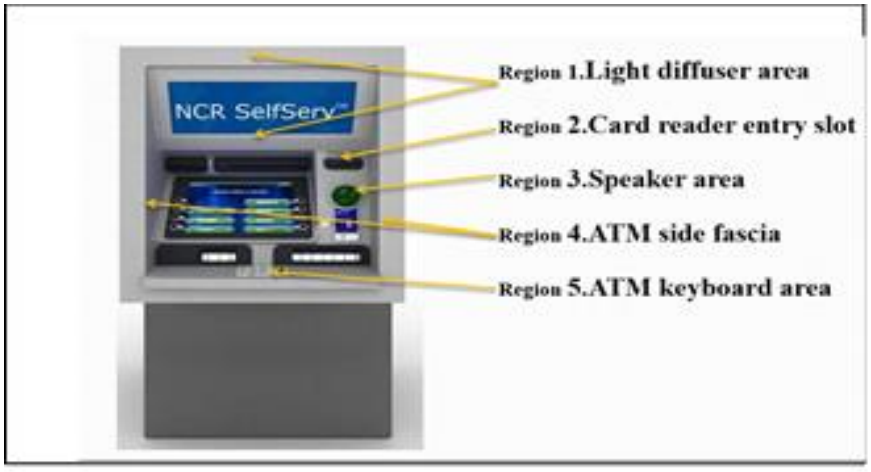

Figure 7: Skimming Device Location [Source: NCR University]

2.2.7.2 Eavesdropping Skimming Attack

A new type of skimming attack called Eavesdropping Skimming has emerged and expanded predominantly in the United Kingdom. The attack targets ATM motorized card readers on older model of the ATM called personas. However, in the USA this attack occurred on the newer model of ATM called SelfServ [5]. The attacker penetrates the ATM facial to have access to the Card Reader of the ATM. A skimmer is then fitted directly onto an electrical node that carries cardholder data on the card reader. On Personas ATMs, the attacker targets the card reader electronic control board by creating a hole behind the ATM card orientation window. In the newer attacks against SelfServ model ATMs, the attacker has changed the method but has maintained the principle. The variance in the way this attack is performed on the two different ATM series shows how sophisticated ATM cyber-criminals are. The ATM SelfServ model targeted is the 6634, which is a Through-The-Wall (TTW) ATM. The attacker makes a hole in the side panel in between the ATM monitor and the card reader. The attacker uses this hole to fit an Eavesdropping Skimmer beneath the card reader connecting directly to the magnetic read head. The hole that was made in the ATM is then concealed by fixing a panel which is the same color as the ATM facial over the entire side panel of the ATM.

2.2.7.3 ATM Card Shimming Attack

ATM card shimming attack is a Man-in-the-Middle attack in which the cyber-criminal inserts a device into the ATM card reader that intercepts and records the data flowing between the EMV chip and the ATM card reader [6]. This data could then possibly be reused to clone a magnetic stripe card. EMV chip data and magnetic stripe data have different check values (CVVs) and therefore the data that is captured from the EMV chip card can't be used to clone a magnetic stripe. Card Shimming is neither a vulnerability with a chip card, nor with an ATM. It is therefore not necessary to add protection mechanisms against this form of attack to the ATM. If the proper authorization procedure is followed during an ATM transaction, counterfeit cards can be immediately detected. This attack can only be successful if an issuer neglects to check the CVV when authorizing a transaction. All issuers must therefore make these basic checks to prevent this category of fraud.

2.2.7.4 ATM Card Trapping Attack

ATM Card Trapping steals the physical card itself through a device attached to the ATM. Cyber-criminals place a device directly over or into an ATM's card reader slot. These devices are designed to capture cards after customers' insert them. In a magnetic stripe environment or chip-and-signature environment, the PIN does not need to be compromised and therefore having an ATM card is enough to compromise a customer's account. Contactless capability can help against this fraud. For example, National Cash Register one of the world's ATM giants helped launch the world's first tap and PIN ATM with ANZ using SelfServ 23 and EMV contactless technology.

2.2.7.5 ATM Cash Trapping Attack

Cash Trapping is where the cyber-criminal uses a device to physically trap the cash that is dispensed and comes to collect it once the customer has left the ATM location [7]. This fraud involves placement of money traps or false presenters in front of the ATM dispenser. When processing a transaction, an ATM dispenses notes into the trap set by cyber-criminals rather than present the money to the customer. The customer assumes the ATM has malfunctioned and leaves. The cyber-criminal then returns, removes the money trap or false presenter, and leaves with cash that was intended for the customer. Cash trapping however mostly succeeds with insider involvement. ATM owners must put measures in place that helps mitigate insider threats like Somewhere you are authentication factor.

2.2.7.6 Transaction Reversal Fraud

Transaction Reversal Fraud involves the creation of an error that makes it appear as though the cash has not been dispensed [8]. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction message. This type of attack has occurred in a number of countries including United Kingdom, Ukraine and Canada [8]. The attacker achieves this by creating a fault on the ATM during a cash dispense operation causing the host switch to reverse the transaction. The account will not be debited although the criminal will remove the cash from the ATM. To avoid being caught, attackers use stolen or skimmed cards. The attacker targets TTW ATMs like the NCR 6634 and 6625. The attacker causes an error on the card reader during a cash dispense operation. The correct PIN is entered and cash requested. After the transaction is authorized by the host switch, the ATM counts the cash and positions it behind the cash dispenser shutter awaiting

to be dispensed. The card is ejected and the attacker waits for the ATM transaction to time out and attempt to capture the card. At this point the attacker holds the card and prevents it from being captured and then forces the cash dispenser shutter open and removes the stacked cash. The ATM reports a card jam and reverses the transaction.

2.2.7.7 Social Engineering/Phishing Attacks

The Victim is tricked into revealing his/her authentication information (PIN) [9]. It can be physically or through electronic means. e.g., rogue websites are set up by the perpetrators to collect authentication information from un-suspecting customers in the name of necessary updates or changes being carried out by their 'Bankers'. The user ends up divulging his card sensitive data to the rogue site.

2.2.7.8 Operational Fraud

The ATM dispenser is manipulated in this type of fraud. The ATM is configured to dispense big denominations as smaller ones, there-by giving out more money than should be dispensed. This can be achieved by either loading wrong denomination notes in the wrong money cassettes or by making a wrong configuration in the software.

2.2.7.9 Malware Attacks

Malware attacks are usually easier with insider involvement as physical access is necessary to deploy the virus. However, this attack is possible online today. The malware file or device is placed on the ATM; its control device is then triggered to give remote control to the perpetrator through a custom interface which enables capture of card numbers and PINs through the private memory space of transaction-processing applications installed on a compromised ATM. Magnetic stripe cards are very vulnerable to this type of attack. Deployment of effective anti-malware software can help mitigate this class of attack.

2.2.7.10 Man-in-the-Middle Attack

In 2015 a "Man-in-the-Middle" network attack was detected in Mexico and ATM operators were Alerted [10]. This class of attack occurs when malware is placed within the banks network and compromises the banks network infrastructure. The network traffic is monitored and the malware listens for transaction messages from the ATMs. When the malware recognizes a cash withdrawal transaction message from a bank card, it intercepts the corresponding host response from the ATM

switch and changes the authorized dispense amount to a larger sum than requested and approved by the ATM switch. In order to perform the fraud, an attacker will initiate a withdrawal transaction at any ATM on the compromised bank network. The attacker will use a pre-defined known card number. The transaction will be intercepted and the card number will be recognized by the malware. It will then wait for the host response to the withdrawal request. The malware will intercept the host response message and modify it to a larger amount therefore the ATM will dispense far more money than what is debited from the account. A variation of the attack, is where the malware intercepts the request, and returns an authorization message such that the transaction host is unaware of the request.

2.2.7.11 Ransomware Attacks

A serious malware called "WannaCry" has impacted many organizations worldwide. This type of threat is known as ransomware. It was launched on 12th May 2017 and targeted computers running Windows 7 or earlier in over 150 countries [11]. WannaCry encrypts the files on end-points that are running Microsoft operating system software, rendering them inaccessible. The files are only decrypted upon payment of a sum of money known as ransom. This malware attempts to infect other end-points on the same network. The malware does not specifically target Banking and Retail systems or their functionalities but ATMs like any other Windows based system are also at risk of this attack. There have been unconfirmed media reports that some ATMs in India having experienced this attack. Customers running any Windows OS who have not applied the Microsoft security patch MS17-010 are at risk. In March 2017 ATM manufacturers advised its customers to deploy this patch.

DieboldNixdolf, another ATM giant recommends the use of Terminal Security to disrupt the execution of malware. Terminal security has more than one protection mechanism which includes sandboxing & application behavior whitelisting, extensive buffer overflow protection, memory access protection and DEP protection. For organizations not running Terminal Security Suite, they can use several general guidelines to prevent such attacks:

I. Prevention of infection via phishing emails by implementation of technical and organizational measures,

II. Segment and secure local area network(LAN)/ virtual LAN(VLAN) with intrusion detection and prevention mechanisms to avoid infection and distribution of malware via the network,

III. All systems should be patched with the latest security patches i.e Microsoft fix MS17-010 (for currently supported Windows OS versions) and emergency fix1 for Windows XP,

IV. All unused services must be deactivated.

Many organizations worldwide have been impacted by another malware called Petya [12]. This malware encrypts the files on end-points running Microsoft operating system (OS) software, rendering them inaccessible. ATMs are at risk of this attack as they run on Microsoft operating systems. All ATMs running any windows OS which has not been patched with the Microsoft security patch MS17-010 are at risk. If any ATMs are infected/locked with the ransomware, then every other ATM and end-point on the same network must be checked for infection as well. Once the malware infects one end-point on the network it will replicate itself to other vulnerable systems.

2.2.7.12 ATM Jackpotting Attack

The term ATM Jackpotting comes from the term Jackpot. In this type of attack, cyber-criminals get huge sums of money from the ATM at once. Cyber-criminals use two methods to perform this attack:

I. **Black Box Attack**: In 2017 NCR warned of a number of Black Box attacks in the UK targeted at Through-The-Wall (TTW) NCR SelfServ ATMs [28]. Some of the attacks have been successful. The cyber-criminal needs physical access to the ATM top cabinet which hosts the ATM PC Core and then puts the ATM in supervisor mode. The attacker removes the ATM network cable so that the ATM cannot be monitored by the ATM monitoring desk. The attacker then installs a black box which is a special device programmed to control the ATM cash dispenser. The ATM goes in supervisor mode for the ATM customer but the cash dispenser still remains working. A black box can be controlled wirelessly through a basic smart phone. The attacker uses the smart phone to issue commands for the ATM to dispense cash. The command can be issued continuously until the ATM cash dispenser runs out of money. The attackers then remove the black box device and leaves no trace of it having been installed on the ATM. In previous Black Box attacks against lobby ATMs, the criminal has gained access to the ATM internal infrastructure by opening the top box. TTW ATMs can be attacked by

breaking through the fascia in this new attack vector. This is done by drilling holes in the fascia such that the ATM screen can be removed. This removal allows enough access to an internal USB hub where the attacker can connect a Black Box and operate the attack from the street. Other TTW ATMs however have a provision to be opened from the ATM facial and the PC core can be accessed. This attack can take less than ten minutes to completely empty the ATM cash cassettes [28]. Investigators have reported in court documents that one suspect got away with more than US$267,000 in just four days. The Secret Service says criminals have already jackpotted more than US$3.5 million from ATMs in the USA [7]. This crime is spreading from state to state in the USA and outside the USA and has affected banks in Massachusetts, Ludlow, Attleboro, Danvers, Boston, London, Germany, Italy and Mexico [29] [30] [31]. This crime is spreading very fast and will soon hit other countries globally if ATM owners do not put in preventive measures [31]. A Supervisory Special Agent with the U.S. Secret Service stated that this crime is likely being carried out by an international criminal group.

II. **Malware Attack**: Malware can be delivered physically by using ATM USB ports or remotely via a compromised banking network. Using a keyboard and command line, the attacker executes the malware. These actions can even be automated so that the malware will work autonomously. The attack can be conducted through the network without physical access to the ATM. The attack is possible when there is no ATM malware protection system, no software whitelisting for the ATM and no authentication is in place for the data exchange between the ATM hardware units and its main application.

2.2.7.13 Smart Card Attacks

Smart cards offer better authentication than passwords, especially in combination with another authentication factor, such as a PIN. However, smart cards are also vulnerable to attacks. A side channel attack is a passive, non-invasive attack to observe the function of a device. If the attack is successful, the attacker can gain valuable information, such as: an encryption key to retrieve data on the card.

2.2.8 PCI DSS

Prior to the PCI DSS, payment card industries, including MasterCard, Visa, American Express, JCB, and Discover, relied on individual policies for the secure processing and storage of credit

card information. Prior to the first release of the standard, the Security Standards Council was established for the payment card industry. The PCI Security Standards Board combined the various guidelines and resulted in the release of version 1.0 of the PCI DSS standard in December 2004. As a result, procedures were put in place to mitigate against sensitive payment card infringements by ensuring that merchants accepting this data know and apply the necessary security measures [32].

The early publications of the American Bar Association [33] and recent studies by [32] and [34] point to a growing climate of concern over the protection of sensitive individuals' credit card information which has led to the development of PCI DSS by MasterCard and Visa, in order to mitigate the problems associated with the secure handling of cardholder data. An important feature in the early stages of the drafting of the standard was the need for compliance and the importance of clarity in terms of process and documentation. This first phase of standardization included many flaws that were later fixed in version 1.2.1 and included many additional requirements to address these issues; virtualization and encryption methods, which increase security [35].

2.2.8.1 DSS 2.0

PCI DSS 2.0 was introduced in 2010 and became the industry standard in 2011. The PCI DSS 2.0 standard did not introduce any significant changes compared to PCI DSS 1.2.1, but included improvements that are subtler and practically suitable for technological progress and safety. The research by [32] documented these differences and highlighted important changes, in particular with regards to wireless networks such as WEP authentication, which was considered unacceptable.

As useful as this standard was, vulnerabilities in PCI DSS 2.0 occurred and could still prevail in the updated standard. For example, Blackwell [36] emphasized the importance of auditing organizations and warned that it could be circumvented by the physical access of employees to many critical systems. The PCI Security Standards Council then provided important guidance on requirements and resources that could be used to identify potential vulnerabilities [37]. For businesses that comply with the PCI DSS 2.0 standard, these guidelines are welcome but lack implementation details and other sources. For example, the standard highlights the areas that are vulnerable to security breaches and helps merchants customize their systems so that their

implementation is easier, to ensure compliance. Although the PCI Security Standards Council [37] effectively describes the objectives of PCI DSS, it does not provide sufficient research or feedback from traders on how to achieve these goals.

2.2.8.2 PCI DSS 3.0

The PCI DSS standard for payment cards is intended to improve the security of cardholder data. This is required when storing or processing cardholder data or authentication data [38].

PCI DSS 3.0 was issued by the PCI Security Standards Council (PCI SSC), a panel of five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc [39]. PCI DSS also includes security requirements of data security and associated audit methods. In particular, the primary account number (PAN) is the determining factor for the applicability of the PCI DSS requirements.

The primary purpose of the PCI DSS is to protect the privacy of cardholder data. Confidentiality as an integral part of the information security triad, which includes integrity and availability, is one of the primary goals of information security and information protection. Confidentiality measures often protect integrity as well. For example, if the data is compromised by an attacker or by malicious software, integrity is often compromised as well. Availability is guaranteed by the systems and infrastructure, which are ready to use and have sufficient capacity to handle all requests as quickly as necessary. Hackers can reduce the availability of information by flooding the system with service requests and, as a result, causing a denial of service attack that prevents access to critical information or data.

Credit card companies need to set up a PCI DSS compliant environment, otherwise a significant portion of their business model would not be feasible and significant losses would be incurred. In addition, credit card companies can expect a loss of reputation and possible fines. The credit card companies are divided into four levels of merchant compliance (levels / tiers 1-4), based on the number of transactions affected within a 12-month period. Each level has specific PCI DSS compliance requirements. Tier two to four companies must complete an annual self-assessment (SAQ) questionnaire and conduct a quarterly network analysis by an approved scanning vendor (ASV) [39]. Companies with a minimum transaction value of US$ 6 million per year are

considered Tier 1 and must produce an annual compliance report and be audited by a qualified security assessor. The result of the test is documented with a Certificate of Conformity.

PCI DSS in Table 1 has 12 key requirements for control measures that are divided into different elements, including network (requirements 1 and 2), cardholder data protection (requirements 3 and 4), Vulnerability Management program. (Requirements 5 and 6), Access Control Measures (Requirements 7, 8, and 9), Network Monitoring and Testing (Requirements 10 and 11), and Information Security Policy (Requirement 12). Each requirement is then subdivided into sub-requirements and testing procedures.

Table 1:PCI DSS Principles and requirements [35]

	PCI DSS Principles	PCI DSS Requirements	
1	Build and maintain a secure network	i.	Install and maintain a firewall configuration to protect data
		ii.	Do not use vendor-supplied defaults for system passwords and other security parameters
2	Protect Cardholder Data	iii.	Protect stored cardholder data
		iv.	Encrypt transmission of cardholder data across open, public networks
3	Maintain a Vulnerability Management Program	v.	Use and regularly update anti-virus software or programs
		vi.	Develop and maintain secure systems and applications
4	Implement Strong Access Control Measures	vii.	Restrict access to cardholder data by business need-to-know
		viii.	Assign unique ID to each person with computer access
		ix.	Restrict physical access to cardholder data
5	Regularly monitor and test networks	x.	Track and monitor all access network resources and cardholder data
		xi.	Regularly test security systems and processes
6	Maintain an information security policy	i.	Maintain a policy that addresses information security for employees and contractors

Compared to version 2.0, version 3.0 includes changes in the form of additional clarifications, guidelines, and advanced requirements. The 20 advanced requirements aim to increase awareness, flexibility and safety.

2.2.8.3 Identified Problems with PCI DSS 3.0

[40] states that there are no clear contrasts between PCI DSS 3.0 and its predecessor. [40] asks if minor changes to the PCI DSS 3.0 standard are sufficient to reduce the number of credit card frauds on the Internet. He further that the clarifications in the new standard appear to be more important than improving the mitigation techniques, and that more than clarifications need to be implemented to effectively protect the cardholder data. Although [40] has a document that provides a very detailed look at the new standard, there is currently little information about PCI DSS 3.0, but there are few documents that substantiate or challenge this view. Although the reasoning of [40] is logical, there is no data to support the hypothesis. The PCI DSS 3.0 standard is a clarification of the PCI DSS 2.0 standard, and is shown in the list of the PCI Security Standards Council [37]. However, this does not mean that there is no change between the standards and that it may be premature to compromise the effectiveness of the standards at such an early stage.

2.2.8.4 The Importance of the Payment Card Industry Data Security Standard

Recent research by [41] has highlighted the proliferation and rapid spread of online credit card payments while highlighting the importance of credit card payments.

The payment card industry is concerned with the protection of cardholder data. Of concern was the growing incompatibilities between PCI and the variety of vendor systems and networks. While investigations are currently underway to address privacy breaches in the public and private sectors, PCI DSS remains the only standard that has been formally implemented to protect credit card holder data [41] and emphasized the importance of effective security to protect cardholder data. Although the total value of card payment transactions exceeds US$ 21 trillion a year, it is unfortunately masked by losses of more than US$ 11 billion from fraudulent transactions. This underscores the importance of PCI DSS as it is the only payment security standard that has been used so far. Therefore, its effectiveness is of the utmost importance if the protection of cardholder data is to be given priority. Failure to comply with these standards is subject to significant financial penalties.

2.2.8.5 Implications of Non-Compliance

PCI DSS is not just important for privacy but there are consequences for non-compliance. [42] examines the impact of violations when suppliers found to be noncompliant due to a crime are subject to fines and / or the introduction of new online editions. An important issue is highlighted in this context, as non-compliance can result in fines of up to US$ 500,000 per crime [43]. In addition to standards, requirements and recommendations, there are already legal and regulatory framework conditions for data protection. As a sector study [44], [45], [46] indicates, non-compliance is the leading cause of data breaches and a lack of awareness and understanding seems to be the main cause of non-compliance. However, PCI DSS 3.0 aims to eliminate this confusion by applying employee training methods to the updated requirements. This awareness is essential for improving security when processing sensitive payment card information.

2.2.8.6 PCI DSS and Legislation

When adopting PCI DSS requirements, traders should also be aware of other laws that may affect their implementation. The Governance, Risk Management and Compliance (GRC) framework is therefore of some value and takes an international perspective on the application of measures to ensure compliance with all required standards, laws and legal implications. In Ireland, for example, the framework provides a mechanism for taking account of the Data Protection Act (DPA) and, at European level, the 'Regulation on Confidentiality of Electronic Communications Networks and Services', which states that consumers are made aware of this and the storing of their data [47].

In the context of increasing security trends that point to an escalation of data backgrounds specifically targeting consumer data [44], [45], [46]), it is important to understand the importance of APD 2011 commerce site in relation to the Compliance with regulations.

2.2.8.7 Data Breaches

According to [48], data from 2005 to 2010 on the spread of attacks on organizations that store sensitive data on payment cards show the significant financial impact of data breaches [48] . It also provides information on many major violations, such as TJX, that have led to changes in the standard. The worrying trend of selling fraud-related information is a cause for concern. The cost of a data breach exceeds the costs of compliance and credit card violations. On this basis, it is important to note that PCI DSS 3.0 must provide complete security to merchants and consumers.

In the context of increasing security trends that point to an escalation of data backgrounds specifically targeting consumer data [44] [45], it is important to understand the importance of APD 2011 commerce site in relation to the Compliance with regulations.

2.2.8.8 Comparison of PCI DSS to other Information Security Standards

I. Big Five Information Security Management Standards

It is undeniable that information is of great importance to a business today. Therefore, protecting information assets is very important and is a top priority for many organizations today.

There is no single formula that guarantees 100% information security. Therefore, it is necessary to have a set of benchmarks or standards in place to ensure that the best security practices are used and that an adequate level of security is achieved.

The five major information security standards are namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. We will discuss their respective strengths, focus, main components and their adoption based on Information Security Management Standards (ISMS). An ISMS is a systematic approach to managing a company's sensitive information so it remains secure. It includes people, processes and IT systems through the application of a risk management process [49]. It can help small, medium and large businesses of all industries protect their information assets.

II. ISO 27001

ISO 27001 is an internationally recognized standard for managing the security risks of information. With ISO 27001 certification, an organization can prove to its customers and other stakeholders that it manages the security of their information. ISO 27001: 2013 (the current version of ISO 27001) contains standardized requirements for an Information Security Management System (ISMS). The standard adopts a process-based approach to set up, implement, operate, monitor, maintain, and improve the information management system. The standard provides a framework for best practices in information security management that helps organizations;

a. Protect information about customers and employees,
b. Effectively manage the risks to the security of information,
c. Comply with regulations such as the General Data Protection Regulation of the European Union (EU GDPR),

d. Protect the brand image of the company.

The ISO 27001 certification is suitable for both large and small organizations in all industries. The standard is particularly useful when information protection is essential, for example in the banking, finance, healthcare, public and computer sectors. The standard is also applicable to organizations that manage large amounts of data or information for other organizations, such as data centres and IT outsourcing companies [50]. Table 2 shows the high level mapping of the 12 requirements of PCI DSS to ISO/IEC 27001:2013 clauses.

Table 2: High Level Mapping of PCI DSS Requirements to ISO/IEC27001 [51]

PCI DSS Requirement	**ISO/IEC 27001 Clause**
1. Install and maintain a firewall configuration to protect cardholder data.	A.12 Operations security
	A.13 Communications security
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	A.12 Operations security
	A.13 Communications security
3. Protect stored cardholder data.	A.12 Operations security
	A.13 Communications security
4. Encrypt transmission of cardholder data across open, public networks.	A.14 System acquisition, development and maintenance
5. Protect all systems against malware and regularly update antivirus software or programs.	A.14 System acquisition, development and maintenance
6. Develop and maintain secure systems and applications.	A.14 System acquisition, development and maintenance
7. Restrict access to cardholder data by business need to know	A.12 Operations security
	A.13 Communications security
8. Identify and authenticate access to system components.	A.12 Operations security
	A.13 Communications security
9. Restrict physical access to cardholder data	A.11 Physical and environmental security
10. Track and monitor all access to network resources and cardholder data	A.12 Operations security
	A.13 Communications security
11. Regularly test security systems and processes	A.14 System acquisition, development and maintenance
	A. 6 Organization of information security
	A.18 Compliance
12. Maintain a policy that addresses information security for all personnel.	A.5 Information security policies

It is recommended to provide better enterprise information security solutions by combining PCI DSS with ISO / IEC 27001 [51]. The flexibility of ISO / IEC 27001 is superior to that of PCI DSS because all controls are written to a high level. See Table 3. Organizations must determine the limitations and applicability of the information security management system to determine their scope. When comparing the scope of the two standards, the scope of ISO / IEC 27001 is selected by the company. However, the size is exactly the same as the data of the credit card holder in PCI DSS. Although the controls of ISO / IEC 27001 are recommendations, it is important to note that the PCI DSS controls are mandatory. ISO / IEC 27001 is more flexible than PCI DSS making it easier to comply with ISO / IEC 27001.

III. BS7799

BS7799 was established in 1995 by the British Standards Institution (BSI) as the standard for the development and implementation of an information security management system, commonly referred to as the Management Information System Security [52]. BS7799 has been designed from the onset as a technology-neutral supplier management system that, when properly implemented, would allow an organization's management to ensure the effectiveness of its actions and its information security features. From the beginning, BS7799 has focused on protecting the availability, confidentiality, and integrity (CIA Traid) of corporate information. This goal remains the main objective of the standard to this day. However, it is important not to talk about protection against all kinds of threats, but only those that an organization considers relevant, and where this is financially and economically justified by a risk assessment.

BS7799 was originally a single standard and had the code of practice status. In other words, it provided guidance to organizations, but was not formulated as a specification that could form the basis of an external verification and certification system. More organizations have begun to recognize the scale, severity and interdependence of information security threats and the emergence of a growing body of privacy and data protection laws and regulations.

The application for a certification option related to the standard began to evolve, which led to the emergence of a second part of the standard in the form of a specification (a specification that uses words such as "must") numbered BS7799-2 (or part 2).

Table 3: Mapping of PCI DSS and ISO/IEC 27001:2013 [53]

Parameter	ISO/IEC 27001:2013 Standard	PCI DSS
Creator	ISO	PCI Council
Flexibility	High	Low
Scope	Depends on the company	Credit cardholders information
Controls applied	Flexible	Tight
Controls	High-level	Low-level
Control types	Should	Must
Compliance	Easy	Hard
Number of controls	114	224
Auditing	Three year cycles and a small-scope audit performed every year	Four network scanning audits and an onsite audit for level 1
Certification	May be given to all companies	Any companies that provide information security for critical paying processes
Compliance level	Does not exist	Exits

The Code of Conduct (using terms such as "may" and controls, not information security management systems) is now under ISO17799 and BS7799-1 (or Part 1). At that time, the relationship between the Code of Conduct and the specification was also established: a specification is the basis of certification systems, and the ISO 27001 standard requires the use of ISO 17799 as a guide to selecting and implementing the controls required by the ISO standard. In fact, ISO 17799 is the second part of ISO 27001. The most recent and applicable version of the Code of Conduct is ISO / IEC 17799: 2005. BS7799-2: 2002 has also been revised and internationalized, and in November 2005 ISO / IEC 27001: 2005 replaced BS7799-2: 2002.

IV. ITIL

The IT Infrastructure Library (ITIL) is a volume library that describes a set of best practices for providing IT services [54]. ITIL has been revised several times in its history and currently consists of five books, each covering different processes and phases of the IT service life cycle. ITIL, currently ITIL v3, focuses on the integration of business and IT. ITIL certifications can be purchased at five levels. ITIL's systematic approach to managing IT services can help organizations manage risk, strengthen customer relationships, implement cost-effective practices, and create a robust IT environment that drives growth, scalability and change.

Developed in the 1980s by the British Government's Central Computer and Telecommunications Agency (CCTA), ITIL originally consisted of 30 books developed and published over time. They included best practices in information technology from many sources (including vendor best practices) around the world.

Over the years, the credibility and benefits of ITIL have been recognized. In 2005, these practices contributed to the ISO / IEC 20000 service management standard, the first international standard for IT service management. It is based on the British standard BS15000. Since 2013, ITIL is owned by Axelos, a joint venture of the Cabinet Office and Capita.

Having a well-managed IT organization that manages the risks and ensures the continued operation of the infrastructure not only saves money, but also allows business people to work more efficiently. ITIL offers a systematic and professional approach to managing IT service delivery and offers the following benefits:

(i) reduction of IT costs,
(ii) improved IT services through the use of proven best practice processes,
(iii) improved customer satisfaction through a more professional approach to service delivery,
(iv) improved productivity,
(v) improved use of skills and experience,
(vi) improved provision of third-party services through the specification of ITIL or BS15000 as the standard for the provision of services in the procurement of services.

According to Axelos, ITIL can also help companies improve their services by:

(i) helping companies manage risks, disruptions and failures,
(ii) strengthen relationships with customers through "effective services that meet their needs",
(iii) establish cost-effective practices,
(iv) build a stable environment where growth, scalability and change are possible.

Table 4 shows the mapping of PCI DSS requirements onto ITIL processes *[55]*.

Table 4: PCI DSS control objectives mapped with ITIL processes [54]

PCI DSS	ITIL
Maintain a vulnerability management program	ITIL service operation availability management, incident management, continuity management
Implement strong access control measures	ITIL service strategy-governance
Maintain an information security policy	ITIL service strategy-governance

COBIT

COBIT 5 provides a comprehensive framework to help companies achieve their GEIT goals. It helps companies get the most out of computing by balancing the benefits and optimizing risk levels and resource utilization. The COBIT 5 family also includes enabler manuals, professional manuals and a collaborative online environment. The most significant change from COBIT® 4.1 is the reorganization of the IT process model framework into an IT governance framework. COBIT 5 process reference model includes processes for GEIT (Figure 8).

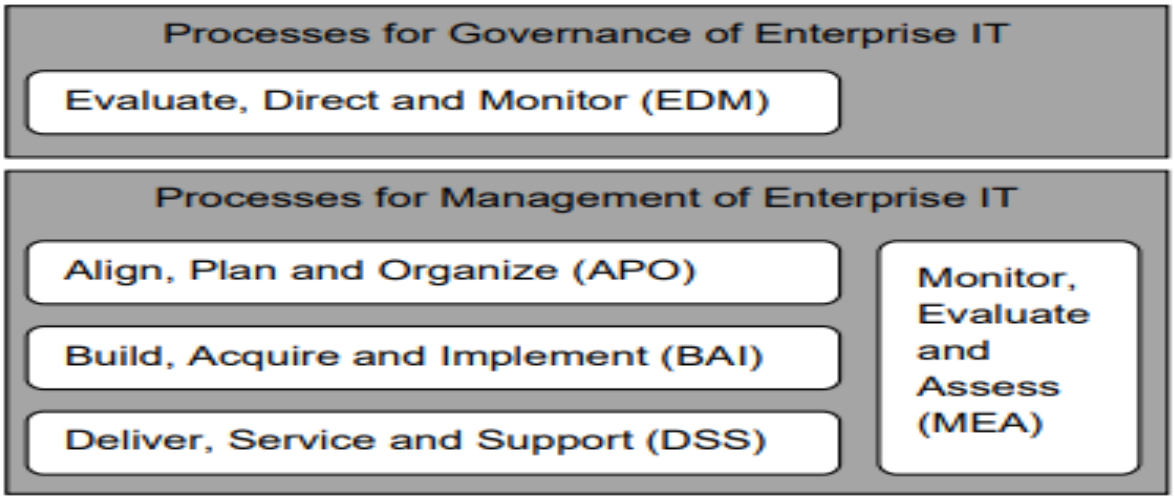

Figure 8: COBIT 5 Process Reference Model [Source: ISACA Website]

V. COBIT Enabling Processes by PCI DSS Topics Network

This section maps the security requirements for PCI DSS 3.0 with the key, associated COBIT 5 enabling processes. All sensitive systems must be protected against unauthorized access from unreliable networks. Firewalls are used for the secure separation of networks. They control network traffic and block unwanted traffic between networks. They can be used locally on workstations or as dedicated systems within the network infrastructure. Using restrictive configurations can reduce the risk of unauthorized access from outside the corporate network.

System failures related to the delivery of systems and components pose a security risk. The passwords and other parameters defined by the system manufacturer are generally available and can be used by unauthorized persons. In addition, many unnecessary services are typically enabled after the initial installation of the operating systems. These services may also be used by unauthorized persons. The main enabling processes of COBIT 5 that can help mitigate risk are illustrated in Table 5.

Table 5: Network Processes [56]

PCI DSS 3.0 Requirement	**COBIT 5 Process**
1. Install and maintain a firewall configuration to protect cardholder data	APO01.08 Maintain compliance with policies and procedures.
	APO03.02 Define reference architecture
	APO12.01 Collect data.
	BAI03.03 Develop solution components.
	BAI03.05 Build solutions
	BAI03.10 Maintain solutions
	BAI06.01 Evaluate, prioritize and authorize change requests.
	BAI07.03 Plan acceptance tests
	BAI07.05 Perform acceptance tests.
	BAI10.01 Establish and maintain a configuration model.
	BAI10.02 Establish and maintain a configuration repository and baseline
	BAI10.03 Maintain and control configuration items
	DSS01.03 Monitor IT infrastructure.
	DSS02.03 Verify, approve and fulfill service requests.
	DSS05.02 Manage network and connectivity security.
	DSS05.04 Manage user identity and logical access.
	DSS05.05 Manage physical access to IT assets.
	DSS05.07 Monitor the infrastructure for security-related events.
	DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	APO01.08 Maintain compliance with policies and procedures.
	APO03.02 Define reference architecture.
	BAI03.03 Develop solution components.
	BAI03.10 Maintain solutions.
	DSS04.08 Conduct postresumption review.
	DSS05.03 Manage end-point security.
	DSS05.07 Monitor the infrastructure for security-related events

Protection of Cardholder Data

Cardholder data should only be stored and displayed under certain conditions. Applicable requirements include storage, deletion, encryption, and masking of data (Table 6). The PCI DSS standard deals with encryption as well as details about the management of electronic keys. When transferring cardholder data to open public networks, encryption is required. When data is transferred (for example, via the Internet, wireless networks, the global mobile communication system [GSM], a general packet radio service [GPRS]), an attacker is more likely to intercept and manipulate the cardholder data. The application of encryption, as indicated, is one of the many methods suggested to minimize this risk.

VI. Vulnerability Management

The use of antivirus software is necessary to protect systems against harmful software. It can include detection techniques based on patterns and behaviours. Model-based detection techniques detect viruses only after updating the new virus model in the antivirus software. Behavioural detection techniques can identify malware based on unconventional patterns of behaviour. However, these detection techniques may be inaccurate and lead to false alarms. The development and maintenance of systems and applications must also be safe. This includes preventing or eliminating vulnerabilities that attackers can exploit to compromise or manipulate cardholder data. Patches need to be installed regularly for operating systems and applications, and secure programming of developments is required. Thorough testing can detect vulnerabilities (Table 7).

VII. Access Control Measures

Access to cardholder data must be restricted to appropriate roles based on the needs of the business. In accordance with the principles of least privilege and the need to know, only persons authorized to access cardholder data for business purposes must be given access. This requires the implementation of controls and authorization management, where each person can be assigned a role with the appropriate permissions (role-based access control [RBAC]) (Table 8). For each person with access to the system, the assignment of a unique identification (ID) is required. This is usually implemented through personal accounts. Only people who can authenticate with a password, token, or other authentication method can access a computer or system. Physical access to cardholder data must also be restricted. Intruders with access to offices or data centres could

Table 6: Processes for Protection of Cardholder Data [56]

PCI DSS 3.0 Requirement	**COBIT 5 Process**
3. Protect stored cardholder data.	APO01.06 Define information (data) and system ownership.
	APO01.08 Maintain compliance with policies and procedures.
	APO13.01 Establish and maintain an information security management system (ISMS).
	APO13.03 Monitor and review the ISMS.
	BAI08.02 Identify and classify sources of information.
	BAI08.05 Evaluate and retire information.
	BAI09.02 Manage critical assets.
	BAI09.03 Manage the asset life cycle.
	DSS01.01 Perform operational procedures.
	DSS04.08 Conduct postresumption review.
	DSS05.03 Manage end-point security.
	DSS05.04 Manage user identity and logical access.
	DSS05.05 Manage physical access to IT assets.
	DSS05.06 Manage sensitive documents and output devices.
	DSS06.04 Manage errors and exceptions.
	DSS06.05 Ensure traceability of information events and accountabilities.
4. Encrypt transmission of cardholder data across open, public networks	APO11.02 Define and manage quality standards, practices and procedures
	APO11.05 Integrate quality management into solutions for development and service delivery.
	BAI03.03 Develop solution components.
	DSS01.01 Perform operational procedures.
	DSS01.02 Manage outsourced IT services.
	DSS01.04 Manage the environment.
	DSS01.05 Manage facilities.
	DSS05.01 Protect against malware.
	DSS05.02 Manage network and connectivity security.
	DSS05.03 Manage end-point security.
	DSS05.06 Manage sensitive documents and output devices.
	DSS06.05 Ensure traceability of information events and accountabilities.

steal, damage, or manipulate media or computer components. The media may be electronic media (such as floppy disks, CDs, and hard disks) as well as paper. With physical access control and visible badges, unauthorized persons can be distinguished from authorized users.

Table 7: Processes for Vulnerability Management [56]

PCI DSS 3.0 Requirement	COBIT 5 Process
5. Use and regularly update antivirus software or programs.	APO12.01 Collect data.
	APO12.03 Maintain a risk profile.
	DSS05.01 Protect against malware
6. Develop and maintain secure systems and applications.	APO12.02 Analyze risk.
	APO12.04 Articulate risk
	BAI03.03 Develop solution components
	BAI03.05 Build solutions.
	BAI03.07 Prepare for solution testing.
	BAI03.08 Execute solution testing.
	BAI03.10 Maintain solutions.
	BAI06.01 Evaluate, prioritize and authorize change requests.
	BAI06.02 Manage emergency changes.
	BAI06.03 Track and report change status.
	BAI06.04 Close and document the changes.
	BAI06.01 Evaluate, prioritize and authorize change requests.
	BAI07.01 Establish an implementation plan.
	BAI07.04 Establish a test environment.
	BAI07.05 Perform acceptance tests.
	BAI07.06 Promote to production and manage releases.
	DSS05.01 Protect against malware.

Table 8: Processes for Access Control Measures [56]

PCI DSS 3.0 Requirement	COBIT 5 Process
7. Restrict access to cardholder data by business need-to-know	DSS05.04 Manage user identity and logical access.
8. Assign a unique ID to each person with computer access.	APO03.02 Define reference architecture.
	APO07.01 Maintain adequate and appropriate staffing.
9. Restrict physical access to cardholder data.	APO01.06 Define information (data) and system ownership.
	DSS05.04 Manage user identity and logical access.
	DSS05.05 Manage physical access to IT assets.

VIII. Monitoring and Testing of Networks

All access to network resources and cardholder data must be tracked, monitored and recorded (Table 9). Logs identify and track unauthorized access. In addition, they are useful for the analysis

of technical errors. PCI-DSS requires logging of all access to cardholder data. Security systems and processes must be tested regularly. This includes a regular analysis of vulnerabilities and attack vectors. These threats must be identified and removed before they can be exploited by an attacker.

IX. Information Security Policy

An information security policy must be created and managed by each company, then communicated to and monitored by all employees (Table 10). It contains information security requirements to which all employees are bound. Information security policy topics include communication of PCI DSS requirements, security awareness training, creation of an incident response plan, and monitoring of the security situation of service providers.

Table 9: Processes for Monitoring and Testing of Networks [56]

PCI DSS 3.0 Requirement	**COBIT 5 Process**
10. Track and monitor all access to network resources and cardholder data.	DSS01.01 Perform operational procedures.
	DSS01.03 Monitor IT infrastructure.
	DSS04.08 Conduct postresumption review.
	DSS05.04 Manage user identity and logical access.
	DSS05.05 Manage physical access to IT assets.
	DSS05.06 Manage sensitive documents and output devices.
	DSS05.07 Monitor the infrastructure for security-related events.
	DSS06.04 Manage errors and exceptions.
	DSS06.05 Ensure traceability of information events and accountabilities.
11. Regularly test security systems and processes.	APO03.02 Define reference architecture.
	APO12.03 Maintain a risk profile.
	APO12.01 Collect data.
	DSS02.01 Define incident and service request classification schemes.
	DSS05.07 Monitor the infrastructure for security-related events.
	MEA01.02 Set performance and conformance targets.
	MEA01.03 Collect and process performance and conformance data.
	MEA01.04 Analyze and report performance.
	MEA02.01 Monitor internal controls
	MEA02.02 Review business process control effectiveness.
	MEA02.03 Perform control self-assessments.
	MEA02.04 Identify and report control deficiencies.

Table 10: Processes for Information Security Policy [56]

PCI DSS 3.0 Requirement	COBIT 5 Process
12. Maintain a policy that addresses information security for all personnel.	APO01.01 Define the organizational structure.
	APO01.02 Establish roles and responsibilities.
	APO01.03 Maintain the enablers of the management system.
	APO01.05 Optimize the placement of the IT function.
	APO01.06 Define information (data) and system ownership.
	APO13.01 Establish and maintain an ISMS.

Companies that store, process, or transfer cardholder data or authentication data must comply with the PCI DSS security requirements. By using COBIT 5, these companies can cover the security requirements of PCI DSS 3.0 with COBIT 5 enabling processes. From another perspective, they can use the security requirements of PCI DSS 3.0 to facilitate implementation of COBIT 5 and achieve the goals of GEIT. In both areas, these synergies help optimize risk and resource utilization.

[57] has defined 11 key controls to be implemented by an organization, in accordance with the information security criteria, by the information security management system standardization body. The controls are called 11EC and are as shown in Table 11. Table 11 also compares the features of the big five ISMS standards.

Information Security Policy: The way an institution expresses its intent with an emphasis on information security means that the governing body of an institution expresses its intention to secure information, guides managers and staff and informs other stakeholders of the priority of the effort.

Communication and Operations Management: Defining organizational security policies to reduce security risks and ensure the correct processing of data, including operations, controls, and clearly defined responsibilities.

Access Control: A system that allows an agency to control access to the areas and resources of a physical facility or a computerized information system.

Table 11: Features of Big Five ISMS Standards [57]

	Key Controls	**ISO 27001**	**BS 7799**	**PCI DSS V2.0**	**ITIL**	**COBIT V4.1**
1	Information Security Policy	√	√	√	√	√
2	Communications and Operations Management	√	√	√	x	√
3	Access Control	√	√	√	√	√
4	Information Systems Acquisition, Development and Maintenance	√	√	√	x	√
5	Organization of Information Security	√	√	√	√	√
6	Asset Management	√	√	√	√	√
7	Information Security Incident Management	√	x	√	√	√
8	Business Continuity Management	√	√	√	√	√
9	Human Resources Security	√	√	√	x	√
10	Physical and Environmental Security	√	√	√	x	√
11	Compliance	√	√	√	√	√

Information Systems Acquisition, Development and Maintenance: An integrated process defining boundaries and technical information systems including capture, development, and the maintenance of information systems.

Organization of Information Security: It is a structure that belongs to an organization in the implementation of information security and includes: the commitment of information security management, coordination of the information security, the authorization process of the information processing equipment. The two main directions are internal organization and external parties.

Asset Management: It is based on the idea that it is important to identify, track, classify and allocate ownership of key assets to ensure their adequate protection.

Information Security Incident Management: It is a program that prepares incidents. From a management perspective, it's about identifying the resources needed to handle incidents. Good incident management also helps prevent future incidents.

Business Continuity Management: Ensuring business continuity under abnormal conditions. The plans promote the willingness of institutions to recover quickly from adverse events or

circumstances, minimize the impact of such circumstances, and provide the means to facilitate their operation during and after emergencies.

Human Resources Security: Ensure that all employees (including contractors and sensitive data users) are qualified and know their duties and responsibilities with respect to their professional duties, and that access is suspended after termination of employment.

Physical and Environmental Security: Measures to protect systems, buildings and related infrastructures from threats that can be adequately protected against their physical environment, buildings and spaces hosting information and information technology systems, in case of damage or unauthorized access to information.

Compliance: This is divided into two areas. The first is respect for the myriad laws, regulations or even contractual requirements that go into the construction of any institution. The second area is compliance with information security policies, standards and processes.

2.2.9 Protecting Mission Critical Assets

Critical assets are the devices, applications, and databases that form the backbone of a business [58]. Without them the business could not work. Therefore, it is logical that the security strategy is multi-layered and plays a role in protecting the critical resources (Figure 9).

There is no consistent approach to securing these assets, as the network and key assets of each company are different. However, if the technology at the heart of the business is known, backups can be prioritized.

2.2.9.1 Layer 1: Perimeter Security

The perimeter is the point at which an organization has control of their network, technology, and data [58]. It must be controlled and safeguarded by the corporation. It is also the first point of contact for many external threats to a network.

There are many technologies available to help an organization secure their network perimeter:

I. Firewalls,
II. Anti-virus / Anti-malware on those firewalls,
III. Intrusion Detection software,
IV. Intrusion Prevention Software,

V. Data Loss Prevention,

VI. Secure De-Militarized Zone (DMZ).

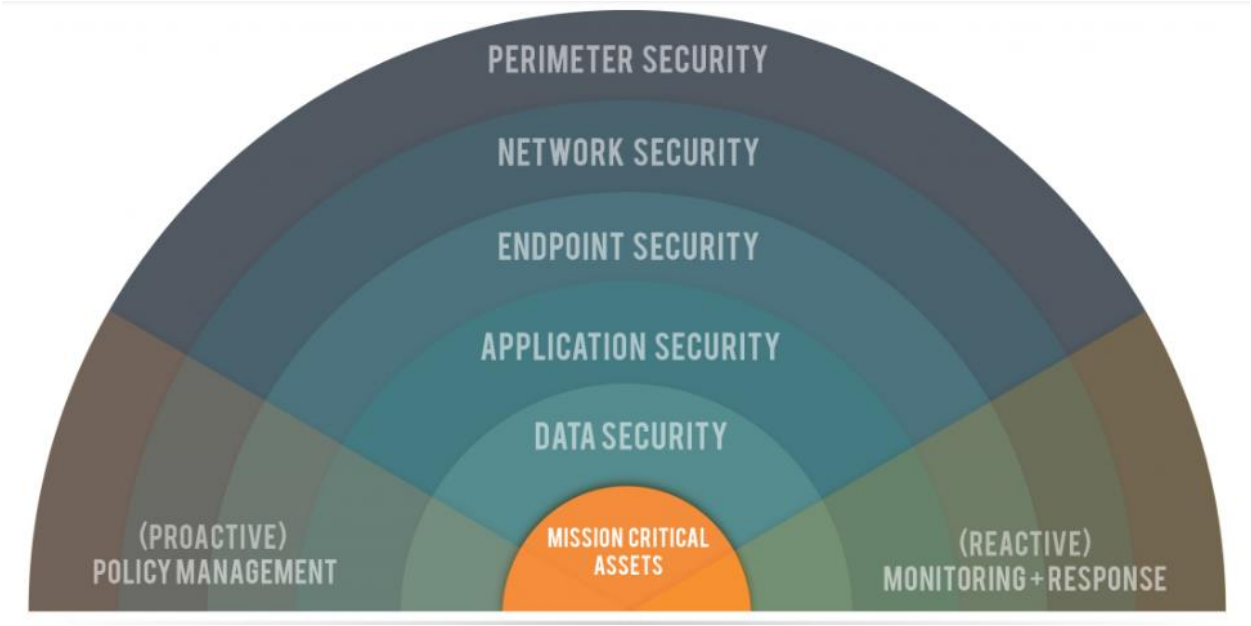

Figure 9: Protecting Mission Critical Assets [58]

2.2.9.2 Layer 2: Network Security

Network security is the securing of a network from other parts of a network. After securing the edge of your network, an organization must understand how to protect the network itself.

These technologies to help secure the network:

X. IDS/IPS: ID/IP with Cisco, Fortinet, AlertLogic - Threat Management (Alertlogic)

I. Network Configuration

II. VoIP Encryption

III. Web Content Filtering

IV. Message Security (SpamSoap)/Spam Filtering

V. Network Access Control (Cisco CSE)

VI. SSLVPN (Remote VPN)

2.2.9.3 Layer 3: Endpoint Security

Endpoint Security deals with any device by which a user accesses data on the network. Endpoint security is particularly critical as even in a moderately sized network, there are many devices connected at any given time. The fact that the devices are often mobile, personal, not encrypted and in an environment with threats makes the situation worse. A BYOD environment is ok when controlled and policies that limit access to corporate data are in place. However, many organizations don't have policies and controls and so BYOD just create more cracks in an organization's security.

It is important to encrypt the "endpoints" on the network, without which, it could pose a significant security vulnerability. Simply put, endpoint encryption is the simplest and most cost-effective way to handle most of the network vulnerabilities in one step. Below are some of the tools that can help with endpoint security:

a. Servers, Workstations, Switches, Routers,
b. Desktop Firewall,
c. Kaspersky, McAfee, Trend,
d. Content Security/AV/Malware,
e. Host IDS/IPS,
f. Endpoint Security Enforcement,
g. AlertLogic,
h. Patch Management,
i. Endpoint/Device Encryption,
j. Mobile Device Management (MDM),
k. 2 Factor Authentication,
l. Hosted Desktops.

2.2.9.4 Layer 4: Application Security

Application security is the process of protecting the software used by an organization to perform a specific function. While each application performs a unique job and business function, each application also has a unique vulnerability. The programs used occupy a "space" in the network.

The network allows users to access the software, and the application also provides access to the network.

Application security is about isolation. Any application hosted on the network or accessible through the network requires controls to prevent the exploit from propagating to the entire environment when exploiting this application. Depending on how the network is designed, application controls can perform the following functions:

(i) Prevent unauthorized applications from running,
(ii) Ensure authorized applications only perform the way they are supposed to,
(iii) Limit access to external web applications.

Another strategy that that be used in Application security is awareness, as prevention is always better than cure.

The tools below can help partition off the applications in a network from the rest of the network.

(i) Software restriction policies and/or software inventory (only approved apps are allowed to run),
(ii) Personal firewalls,
(iii) Controlling through OS,
(iv) Web browser sandboxing,
(v) Database Monitoring,
(vi) Unified threat management through firewall,
(vii) Nextgen firewalls.

2.2.9.5 Layer 5: Data security

Data in organizations is very important and therefore needs to be protected. Data security protects a company's critical files from corruption, tampering, theft and deletion.

Credit card numbers, bank account numbers, social security numbers, medical records, personal information, intellectual property are all examples of data. Even if a hacker had to access a company's database, it is possible to protect the data itself.

Key to Data Security

Data security is about difficult in displaying, reading, editing, and deleting data. Therefore, the main tools for backing up data are generally divided into three categories:

a. File Encryption and Disk Encryption: Encryption is the process of scrambling data so that it can only be read by people with the key.
b. Backups: In addition to theft, the data must be protected from damage. A backup strategy is an essential step in protecting against data corruption.
c. Data Erasure: Any element containing a memory can store data and therefore presents a security risk. When disposing of old devices, whether for distribution to third parties or for distribution to the electronics recycler, the data must be erased properly.

Tools that can be used to protect an organisations data are:

I. Data erasure and cleaning services,
II. Data Drive Encryption / Full Disk Encryption,
III. File encryption software,
IV. Data backups (regular and tested),
V. Two-factor authentication,
VI. Data integrity monitoring,
VII. Management of corporate rights,
VIII. Identity and access management,
IX. Prevention of data loss.

2.2.10 Defence in Depth

Defence in Depth is a practical strategy for securing information security in today's highly networked environments. It is a best practice strategy based on the intelligent application of existing technologies and techniques to ensure Information Assurance [59].

Information Assurance is provided when information and information systems are protected against attacks by the application of security services such as availability, integrity, authentication, confidentiality and non-repudiation. An important principle of the defence-in-depth strategy is that to ensure information assurance, there are three basic elements that need to be focused on: people, technology and operations (Figure 10).

Figure 10: Defence in Depth Strategy [59]

2.2.11 Software Whitelisting

The three core principles (Figure 11) of software whitelisting which mitigates ATM software risks covered in section 2.2.6 are:

The 1st principle is "Only authorized code can run": This is the ability to identify all of the executable code on an ATM, authorize it to execute, and make sure that no other code, such as viruses, worms or Trojans, can execute on that ATM.

The 2nd Principle is "Authorized code cannot be tampered with": This is the ability to ensure that the authorized code is protected from any attempt to tamper with it. Specifically, this means the ATM's code is protected from unauthorized changes, modification, deletion or other types of tampering.

The 3rd Principle is "Authorized code cannot be hijacked": The authorized code that is allowed to run cannot be hijacked, or tricked into doing something it is not supposed to do. This is very important for protecting ATMs from those emerging threats we spoke about, like Buffer overflows and other types of code injection.

Together, these three core principles of software whitelisting ensure that an ATM is always executing exactly the way it was intended to.

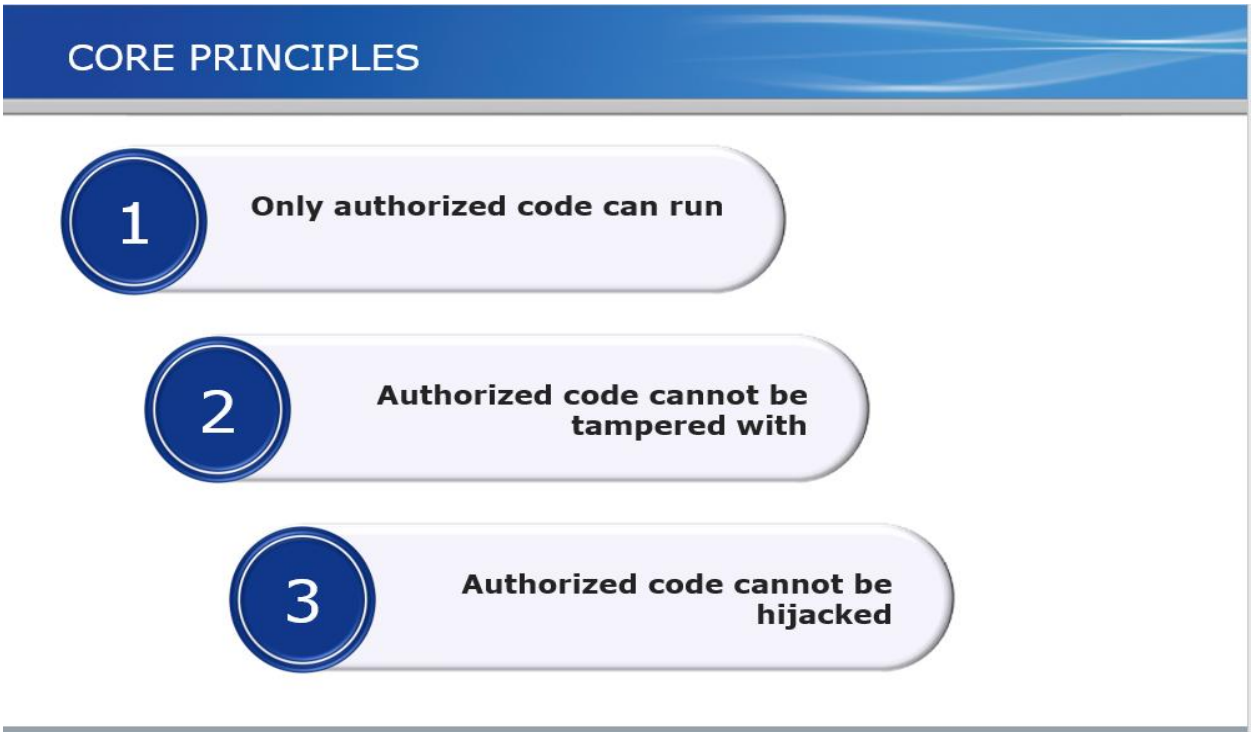

Figure 11: Software Whitelisting Principles [16]

2.2.12 Related Works

Nicho [60] discussed the issues faced in PCI DSS implementation. He explored and evaluated the applicability of the related information system(IS) security and audit frameworks that can be integrated for ensuring an effective and efficient comprehensive organizational IS security and proposed an integrated comprehensive security framework for data protection.

Researchers in [61] reviewed the most common complaints made by merchants and showed that they are mostly based on misunderstandings of the purpose and nature of the compliance procedure to PCI DSS and argued that any company with a sound approach to security should have little problems with the process. It was concluded that if properly understood and applied, the PCI Compliance process can be of real benefit to businesses not just in absolute terms of achieving compliance but as a good starting point in developing a more effective overall approach to security

Richard [62] examined the information-intensive card payment approval process and the security vulnerabilities that emerge as a result of shifting to electronic forms of payments. He explored how criminals gather and use payments information to commit fraud and addressed the monetary harm that fraud inflicts on participants in the payment system. He then reviewed several important

initiatives, in the United States and elsewhere, designed to combat card payment fraud and finally discussed the limited effectiveness of industry efforts to establish payment security standards on its own and the resulting policy concerns.

Matthew [63] proposed incorporating COBIT best practices in PCI DSS for effective compliance and suggested the model needs to be tested in different industry sectors and geographic locations to validate and generalize it.

Jennia and Tzi-cker [64] discussed the pre-requisite for PCI DSS compliance procedure which is to identify the credit card data flow, specifically, the stages of the card transaction processing and the server nodes that touch credit card data as they travel through the organization. He stated that this pre-requisite poses a challenge to merchants and described a tool that is designed to automate the task of identifying the credit card data flow in commercial payment systems running on virtualized servers hosted in private cloud environments.

A comparative study of the big five information management system standards [65] emphasized the importance of protecting information in an organization. It states that no single formula can guarantee 100% of information security and proposes a need to use a set of standards to ensure the best security practices are adopted and an adequate level of security is attained. Different information security standards were briefly introduced and then a comparative study for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT was provided. A picture of the position and specialization of each standard, adoption by countries and their usability levels was also given.

Zrinka presented a model of how to reduce required resources and how to simplify achieving PCI DSS compliance by using ISO 27001 [53]. He stated that all merchants and service providers of e-commerce and card payment service have to be compliant with PCI DSS.

Katerina [66] explored the main barriers and key issues that the hotel industry professionals faces during the Payment Card Industry Data Security Standards (PCI DSS) compliance process and discussed weaknesses and gaps in the PCI compliance process within the hotel industry. It was proposed that understanding these gaps will provide a foundation to develop strategies and methods to address the issues in the future. A list of 20 PCI compliance issues that hotel executives face during the process was compiled as an outcome of the first stage of the study. The second

stage of the study showed high-financial cost of implementation and maintenance, lack of qualified staff, inadequate staff training, ambiguous terms in PCI DSS language, and lack of vendors' support and compliance to be the top five issues in PCI compliance in hotels.

Researchers [67] proposed a new concept that enhances the overall experience, ease of use and convenience of the ATM transaction. Features such as face recognition and one-time password (OTP) sent to a mobile phone were used to improve account security and protect user privacy. Facial recognition technology helps the machine to identify each user in a unique way, turning the face into a key. This completely eliminates fraud by theft and duplication of ATM cards. In addition, the randomly generated OTP frees the user from the memory of the PINs, since it acts itself as a PIN.

Researchers in [68] analysed the existing ATM system by looking at all the issues and challenges that are being faced by ATM users. ATM fraud was the major issue discussed and the researcher recommended to use of biometric feature to enhance ATM security.

A system based on the use of biometric voice access control in automatic teller machine was proposed [69]. In the proposed system, access will be authorized simply by means of an enroll user speaking into a microphone attached to the automatic teller machine. There are 2 phases in implementation of the proposed system: training phase and testing or operational phase.

2.3 Chapter Summary

In this chapter, a comprehensive overview of the background theory behind ATM crime has been given. In particular, ATM threats and risks have been discussed. The chapter has also discussed the PCI DSS in relation to other ISMS. The framework 'Protection of Mission Critical Assets' that has been used in the proposed framework to enhance ATM security has also been covered. The gap that has been found in literature has also been highlighted in this chapter.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Chapter Introduction

This chapter explains the methods and procedures used to systematically collect and interpret data for this research. The chapter discusses the research methods to be used in this study. It contains the research plan to be used, the description of the variables, the location of the study, the target population and the sampling method to be used. It will also cover data collection techniques, the research tool to be used, the data analysis technique and ethical considerations.

3.2 Baseline Study

In this research a baseline study on the level of ATM security in Zambia based on the PCI DSS standard carried out. Extensive literature review was conducted on the problem statement. Abstracts, journals, conference proceedings, government reports, books, the internet and years of experience working maintaining ATMs was used to do background research. This was to gain extensive knowledge in the subject area.

3.3 Hypothesis

A hypothesis about the problem was developed based on the literature reviewed and the experience from working with ATMs. A hypothesis is a tentative assumption made in order to draw out and test its logical and empirical consequences [70]. A hypothesis is important as it provides a focal point of the research. The hypothesis developed in this research is that ATM fraud has continued to be a growing problem in Zambia because commercial banks are not 100% compliant with the PCI DSS framework.

After formulating the hypothesis, a research design was prepared. A conceptual structure was stated that would guide the research.

3.4 Interpretivist or Positivist

Natural sciences generally use quantitative methods and follow the positivist approach, while the social sciences tend to focus on qualitative methods and use an interpretative approach [71]. Positivist researchers believe that there is a reality and that it is possible to quantify it. The researchers make assumptions and test them with the appropriate data to determine whether they

could be supported or not. It is important that research activities do not change and do not influence the reality studied.

The research method of this study is based more on positivist approaches than on interpretative approaches, since we want to use general facts by examining the hypotheses (as they are in the questionnaire questions) and statistical methods.

The overall research issue we focus on is the ATM fraud and how ATM security can be enhanced in Zambia using the PCI DSS.

3.5 Quantitative or Qualitative Research

As mentioned in the previous section, quantitative research methods are generally associated with the positivist approach, while qualitative research methods are generally associated with the interpretive approach.

Quantitative research focuses on numbers and generally uses mathematics and statistics to test hypotheses and explain the results of research. On the other hand, qualitative research devotes more attention to words (descriptive analysis). Words are used to represent the analysis of social phenomena rather than the numerical measure. 'Quantitative researchers typically bring a set of concepts to bear on the research instruments being employed, so that theoretical work precedes the collection of data, whereas in qualitative research concepts and theoretical elaboration emerge out of data collection' [72].

This research is both quantitative and qualitative has it uses questionnaires and interviews to collect data.

3.6 Data Collection Methods

Depending on the type of research carried out, different methods of data collection can be used. It is common practice to combine multiple data collection methods to support the research results. We used questionnaires (combination of closed-ended questionnaires and open-ended questionnaires), semi structured interviews and participant participation as data collection methods. The data collected by the questionnaire was analyzed quantitatively by Microsoft Excel and the transcript of qualitatively recorded transcripts using semi-structured interviews was used as additional evidence for this study.

The items in both the questionnaire and the interviews included the 12 requirements of the PCI DSS standard. The questionnaires had both open ended and closed ended questions. The questionnaire had four sections. The first section deals with participants' profile. The second section deals with participants' use and perceived importance of the ATM, customers security practices on the ATM and also customers awareness on ATM frauds . The third section deals with EMV chip and Pin cards and the last section deals with items derived from the PCI DSS. Participant observation was also used as one of the researchers worked as an ATM engineer for 9 years in charge of both hardware and software maintenance of the ATM.

3.6.1 Semi-structured interview

The semi-structured interview is perhaps the most commonly used type of interview in qualitative social research [70]. In this type of interview, the researcher wants specific information that can be compared and contrasted with information from other interviews. For this, the same questions must be asked in every interview. However, the researcher wants the interview to remain flexible so that other important information can be displayed. For this type of interview, the researcher sets an interview schedule. This can be a list of specific questions or a list of topics to discuss. This is done at each interview to ensure continuity. The ideal interviewees in this research are the people who have experience of working work ATMs and dealing with ATM fraud.

3.6.2 Questionnaires

There are three basic types of questionnaires: closed questionnaires, open questionnaires or a combination of both.

3.6.2.1 Closed Questionnaires

Closed questionnaires are probably the type that most people are most familiar with. Most people have been the subject of long-term consumer surveys that examine their buying habits and allow them to participate in the raffle. This type of questionnaire is used to compile statistics in

quantitative research. Because these questionnaires follow a predefined format and most can be scanned directly into a computer for easier analysis, higher numbers can be generated.

3.6.2.2 Open Questionnaires

Open questionnaires are used in qualitative research, although some researchers quantify the answers during the analysis phase. The questionnaire does not contain check boxes, but the

respondent has an empty space to write an answer. While closed questionnaires can be used to find out how many people are using a service, open questionnaires can be used to determine what people think of a service. Because there are no standard answers to these questions, data analysis is more complex. In addition, fewer questionnaires need to be distributed because of the search for opinions rather than numbers.

3.6.2.3 Combination of the two

Many researchers tend to use a combination of open and closed questions. In this way, it is possible to know how many people are using a service and what they think of this service on the same form. Many questionnaires start with a series of closed questions, with checkboxes or scales to classify, and end with an open question section for a more detailed answer.

3.6.3 Participant Observation

The researchers mainly observe direct observation and participant observation. Direct observation tends to be used in areas such as health and psychology. It involves observing a "subject" in a given situation and often uses technologies such as visual recorders or disposable mirrors. For example, psychologists can monitor the interaction of mother, father, and child in a specially designed playroom with a one-way mirror to better understand family relationships. In participating observation, however, the researcher is much more involved in the life of the observed.

Observing the participants as a research method has been bad news as a number of researchers have become undercover participants in organizations, who participate in their activities without knowing that they are doing research. Obviously, watching participants who know who the researcher is and what they are doing can be a valuable and rewarding method for a qualitative survey.

The researcher worked as an ATM engineer for a period of nine years, before and for the period of the data collection.

3.7 Sampling

There are many different ways to select a sample, and the method used depends on the research field, research methodology, and researchers' preferences. There are basically two main types of

sample; probability samples, purposive samples. Quantitative research assumes that, with a careful selection of the sample using the right method, it is possible to generalize the results across the entire research population. For many qualitative researchers, however, the goal is not to generalize their work to all researchers. Instead, they try to describe or explain what happens in a smaller group of people. The believe, this could reflect the behavior of the broader research group. They however accept that the results of the research could be different if done with a different group of people. In probabilistic samples, all individuals in the research population have a certain chance of being selected. These types of samples are used when the researcher wants to explain, predict or generalize the entire research population. On the other hand, purposive sampling is used when the purpose is a description rather than a generalization. This type of sample cannot determine whether a person will be included in the sample or not.

In the probabilistic and well-founded categories there are several different sampling methods.

3.7.1 Choosing Sample Size

This depends on the type of research being conducted. For large quantitative surveys, you need to contact many more people than a small qualitative survey. The size of the sample also depends on what you want to do with your results. Quantitative studies tend to say that the larger the sample, the more accurate the results. However, this is likely to be limited by time and money. A researcher needs to choose a sample size that is manageable. Extensive quantitative research, uses statistical methods to select the sample size required for a given precision and the possibility of generalization. It is difficult to choose the of participants at the beginning of a research in purposive sampling.

This research deals with eight (8) commercial banks out of the 16 registered commercial banks in Zambia for the first research question. The statistics obtained from BOZ are for all commercial banks in Zambia. The banks that took part in this Research are Barclays Bank, Standard Chartered Bank, Zanaco, UBA, Natsave, Stanbic, FNB and Atlas Mara. Due to the sensitivity of the information being collected in this research and the banks need to maintain their reputation, the banks remain anonymous and have been randomly coded as BANK A, BANK B, BANK C, BANK D, BANK E, BANK F and BANK G. Two (2) ATM vendor companies that banks use to service their ATMs were also selected. One vendor installs, repairs and maintains ATMs on behalf of the banks in Zambia while the other one replenishes money in the ATMs on behalf of the banks.

The participants from commercial banks were the employees in charge of ATM security in the different banks which is Information Technology (IT), IT Risk and IT Security staff for some banks. This is due to the fact that some banks don't have IT security department to secure their infrastructure but use their general IT department to secure the IT infrastructure. This sample was selected as these are the people that understand the operation of the ATMs and the problems surrounding the ATMs. These are the people mandated to secure the ATM infrastructure in order for the banks to protect customer data. 5 participants were selected from each bank expect for Bank A, which only has 2 people in IT departments that are in charge of securing the ATM.

After the sample size was determined an introductory letter was obtained from the Dean of the School (Appendix 1) and circulated to the various Heads of Department in charge of ATM security in the 8 banks seeking permission to collect data for the research. The data collected was used purely for this research and nothing else.

This study was carried out over a period of four months. The items in the instrument were analyzed using descriptive statistical methods.

3.8 Ethical Clearance

An ethical clearance certificate was obtained from Directorate of Research and Graduate Studies (DRGS) at the University of Zambia. An introductory letter was also obtained from the Dean of School of Engineering that was taken to the participating banks seeking permission to collect data from there. The banks were assured of the following:

Anonymity: assurance was given to the participating banks that the information given will not be traced back to the bank. Banks in this this have therefore been coded as BANK A, BANK B, BANK C, BANK D, BANK E, BANK F, BANK G and BANK H.

Confidentiality: information collected has not been availed to any third party and was used exclusively for research purposes.

3.9 Chapter Summary

In this chapter, we addressed the research methods used in this research. We also explained the design of the survey questionnaire and interview questions used based on this study.

CHAPTER FOUR: RESULTS

4.1 Chapter Introduction

This chapter looks at the results of the research that was conducted on eight commercial banks in Zambia; BANK A, BANK B, BANK C, BANK D, BANK E, BANK F, BANK G and BANK H to determine the level of security on ATMs and how ATM security can be enhanced. It also looks at the statistics collected from Bank of Zambia on ATM fraud before and after the introduction of the EMV chip and PIN card.

The survey revealed that the banks are not compliant with the PCI DSS and on average the level of security on ATMs is 66.5 %; the least compliant bank is at 50% and the highest compliant bank is at 83%. The statistics obtained from BOZ revealed that ATM card fraud has continued to rise even after the introduction of the Chip and Pin card.

Finally, the results from baseline study and the statistics from BOZ enabled us to review existing ICT protection frameworks and to propose a framework to enhance ATM security. An existing framework for protection of mission critical infrastructure discussed in 2.2.9 was adopted and modified to add another layer to deal with human security and to add the PCI DSS.

4.2 Baseline Study Results

In this section, we look at the results of the baseline study which was carried out as part of this research, on which the justification to develop and propose the ATM security framework is based.

4.2.1 Survey Results

Microsoft excel (MS excel) application software was used to analyse the data which was gathered from the survey.

1) Gender

The respondents at the 8 commercial banks were as shown in Table 12.

Table 12: Gender

Gender	Frequency	Percentage
Male	31	83.8
Female	6	16.2
Total	37	100

The results showed the gender distribution for the study that was conducted with the commercial banks as 83.8 % and 16.2 % for male respondents and female respondents respectively. The result showed that there was gender imbalance.

2) Age

The distribution of the age of respondents is as shown in Figure 12.

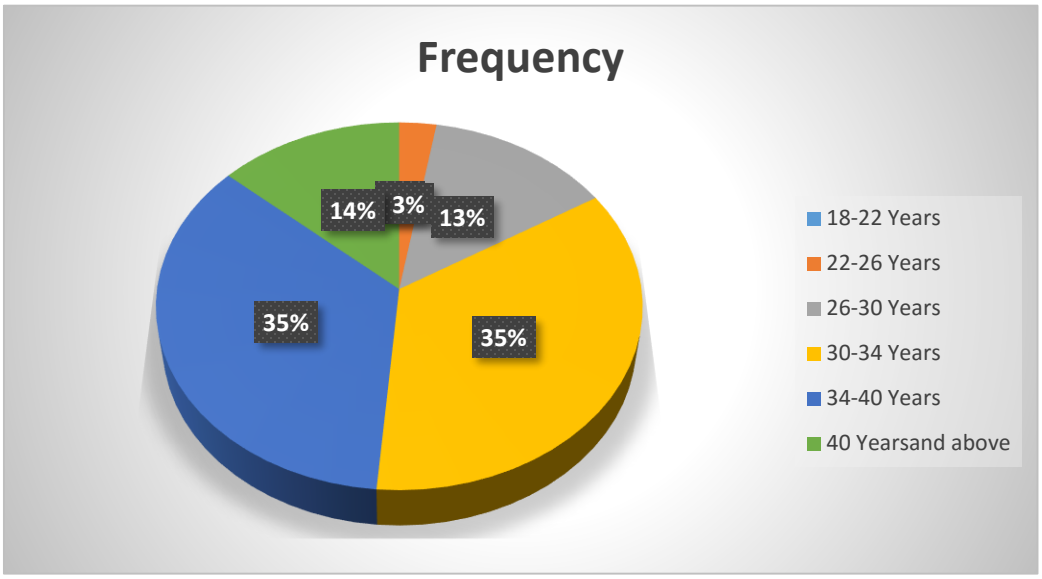

Figure 12:Age of Participants

3) Marital Status

The results showed that 27.1% respondents are single and 72.1% of the respondent are married (Table 13).

Table 13: Marital Status

Marital Status	Frequency	Percentage
Single	10	27.1
Married	27	72.9
Total	37	100

4) Bank Participant Distribution

As can be seen from Figure 13 and Table 14, 2 respondents are from Bank A and Bank B, Bank C, Bank D, Bank E, Bank F, Bank G, Bank H each have 5 respondents. Only 2

participants were selected from Bank A because the bank only has 2 employees in charge of Information Technology and ATM security. The sample size is small because only the employees in charge of ICT security for the various banks were selected. The participants are from IT department or IT security department for the banks that have a separate IT security department.

Table 14: Bank Participation

BANK	No. of Participants
BANK A	2
BANK B	5
BANK C	5
BANK D	5
BANK E	5
BANK F	5
BANK G	5
BANK H	5

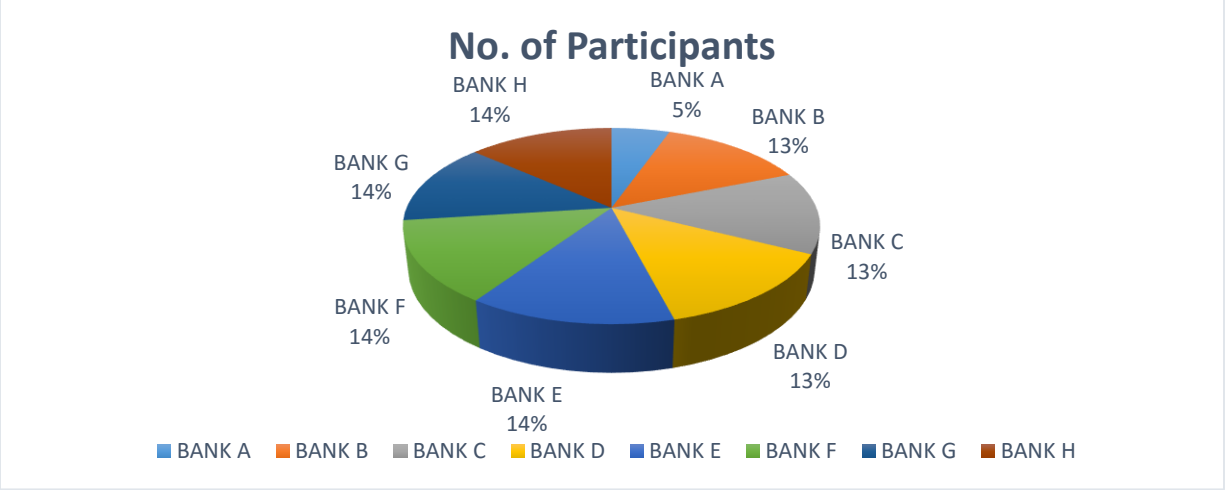

Figure 13: Bank Participation

5) Line of Speciality

As can be seen from Figure 14, 78% of the respondents are IT specialists,14% are IT Auditing specialists and 8% are IT security specialists. From the results it can be seen that most of the commercial banks don't have employees that are dedicated to IT security.

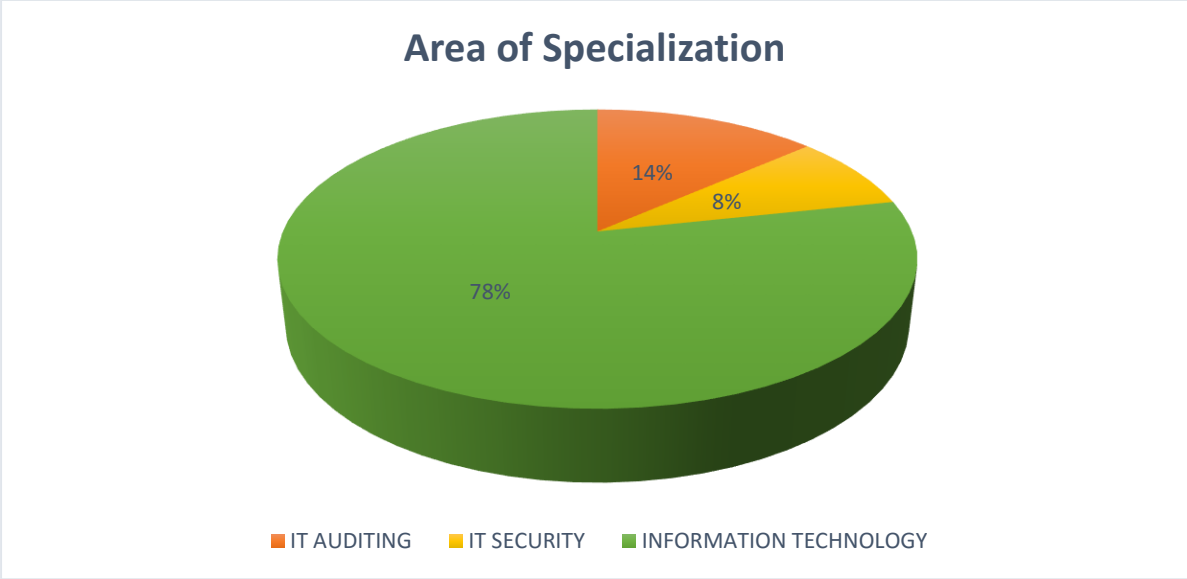

Figure 14: Specialization

6) Customer Perception of the ATM

As can be seen from Figure 15, 100% of the respondents from all the banks believe that ATMs have improved the way banking is performed. This gave us the reason to investigate ATM crime and propose a framework to help enhance ATM security as people believe ATMs are a good thing.

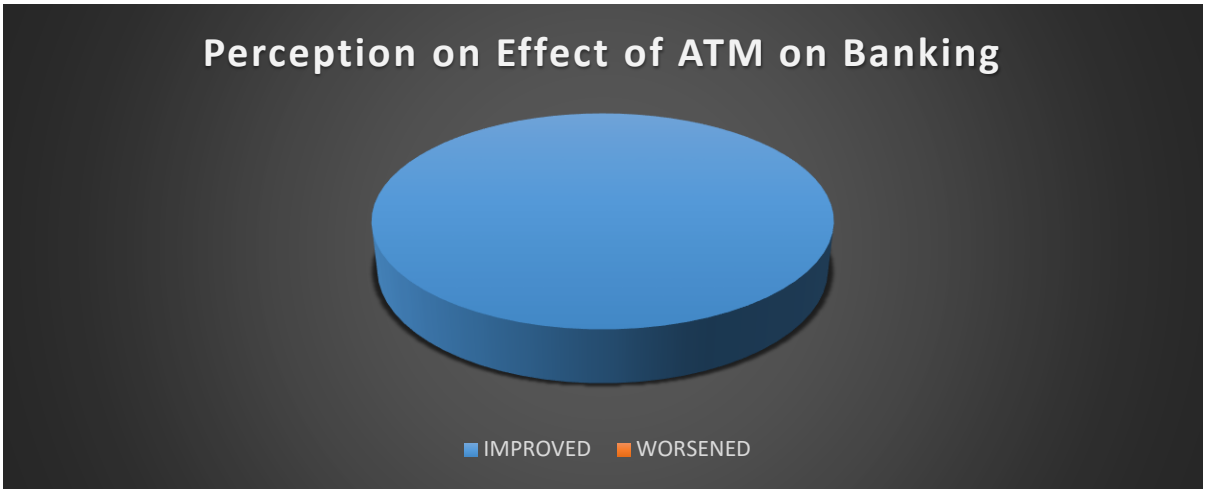

Figure 15: Customer Perception of the ATM:

7) Level of ATM Fraud Exposure

Figure 16 shows that 27% of the respondents use the ATM on a daily basis and are therefore exposed to ATM crime on a daily basis. 68% of the respondents use the ATM once a week and are therefore exposed to ATM fraud once a week. 5% of the respondents use the ATM once a month and the level of exposure to ATM fraud is monthly. The more frequent a card holder uses the ATM, the more the exposure to ATM fraud.

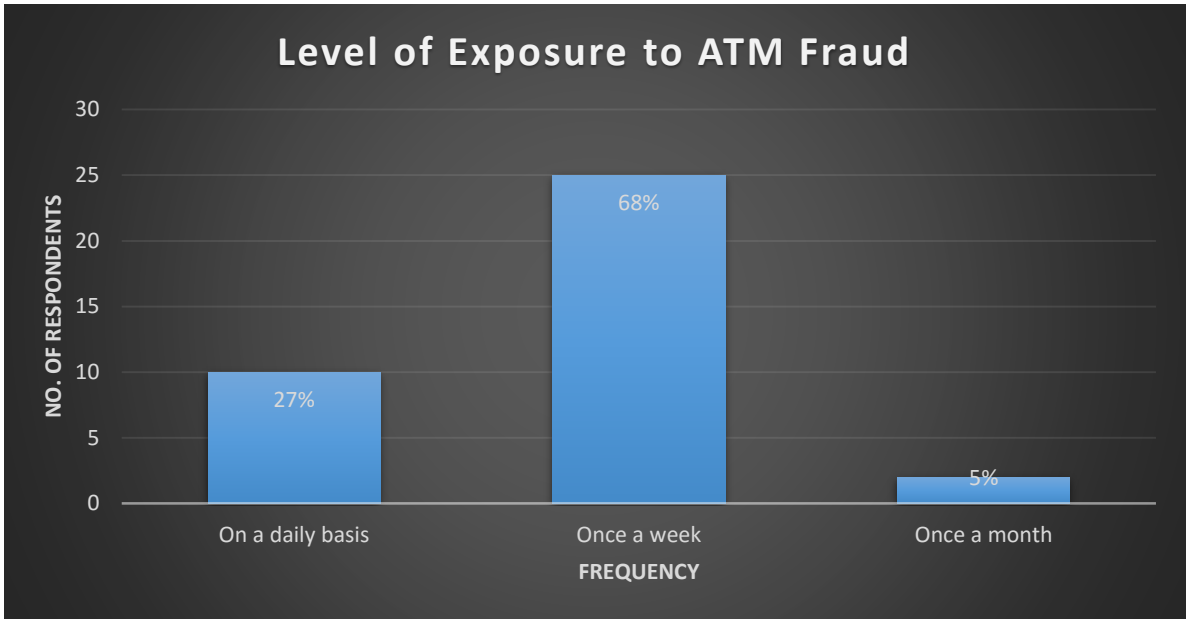

Figure 16: Exposure to ATM Fraud

8) Awareness of ATM Fraud

As can be seen from Figure 17, 100% of the respondents are aware of the existence of ATM fraud. However, the fraud that all the respondents know is the ATM card skimming fraud which is the most common ATM fraud.

Figure 17: ATM Fraud Awareness

9) Awareness of Emerging ATM Crime

As can be seen from Figure 18, only 49% and 35% of the respondents know what ATM card shimming and ATM Jackpotting is respectively. 35% and 32% of the respondents have heard of ATM card shimming and ATM Jackpotting respectively. 16% and 33% have never heard of ATM card shimming and ATM Jackpotting respectively. This is not a good sign as the people that the banks have entrusted with protecting the ATM don't know of the existence of emerging ATM crimes which they should be protecting against.

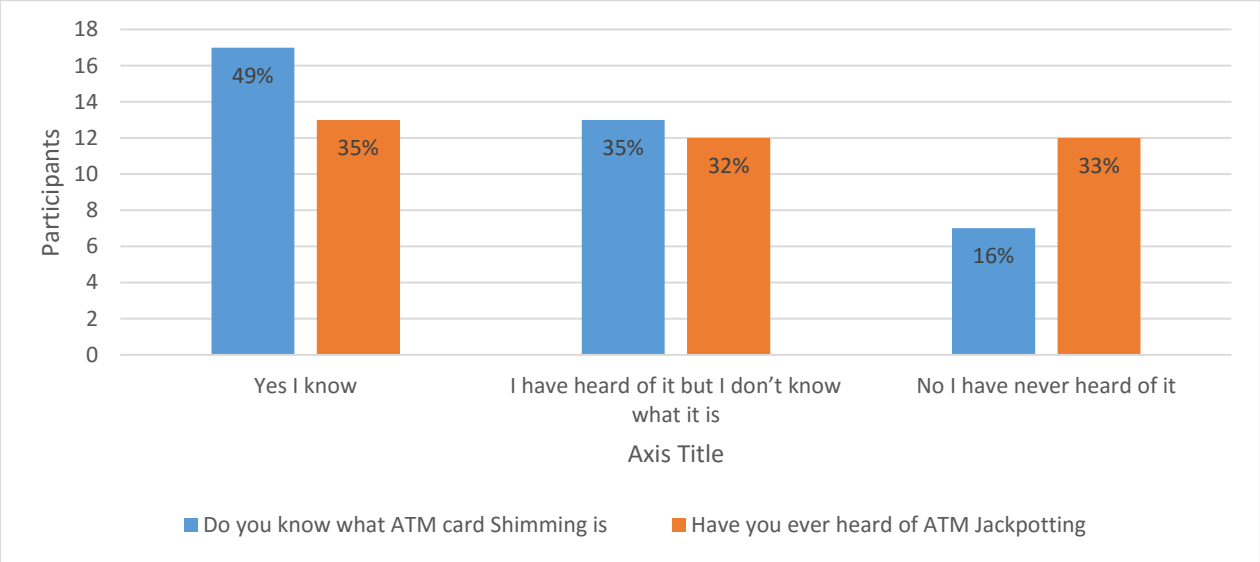

Figure 18: Emerging ATM Crime Awareness

10) Victim of ATM Fraud

From Figure 19, it can be seen that the respondents from Bank A have not been victims of ATM fraud, all respondents from Bank B, Bank C, Bank F Bank G, and Bank H have not been victims of ATM fraud as individual but the banks have been victims of ATM fraud. 1 of respondents from Bank D and Bank E have been victims of ATM fraud while 4 of respondents from Bank D and Bank E have never been victims of ATM fraud.

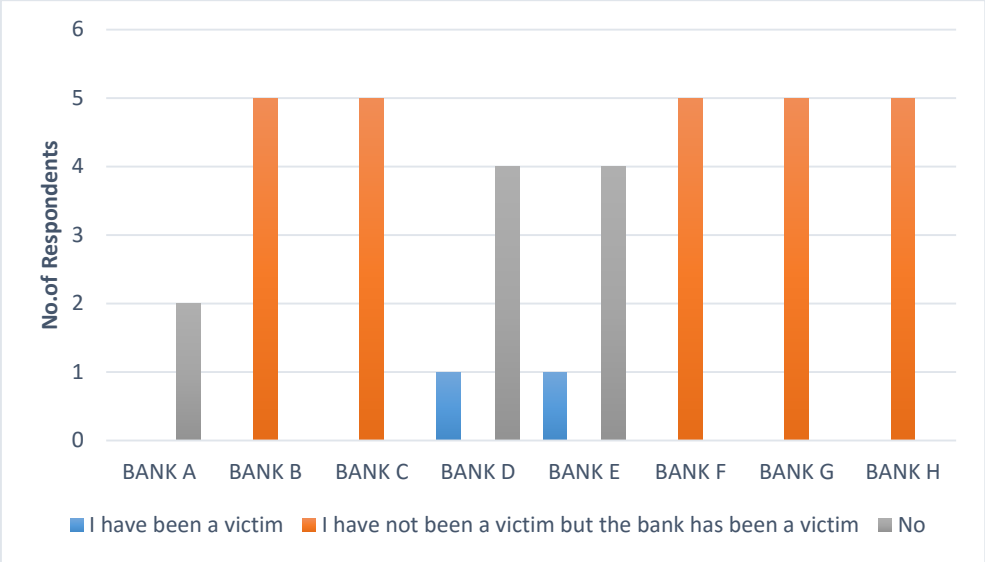

Figure 19: Victim of ATM Fraud

11) Banks Migration to EMV Chip and Pin Card

All the banks have migrated to the Chip and Pin card from the old magnetic stripe card (Figure 20). The new EMV Chip and Pin card has a magnetic stripe on the back of the card. All banks migrated after a mandate by BOZ for all banks to migrate to the EMV Chip and Pin card. This is in a quest to mitigate the ATM card skimming attacks that the country has experienced.

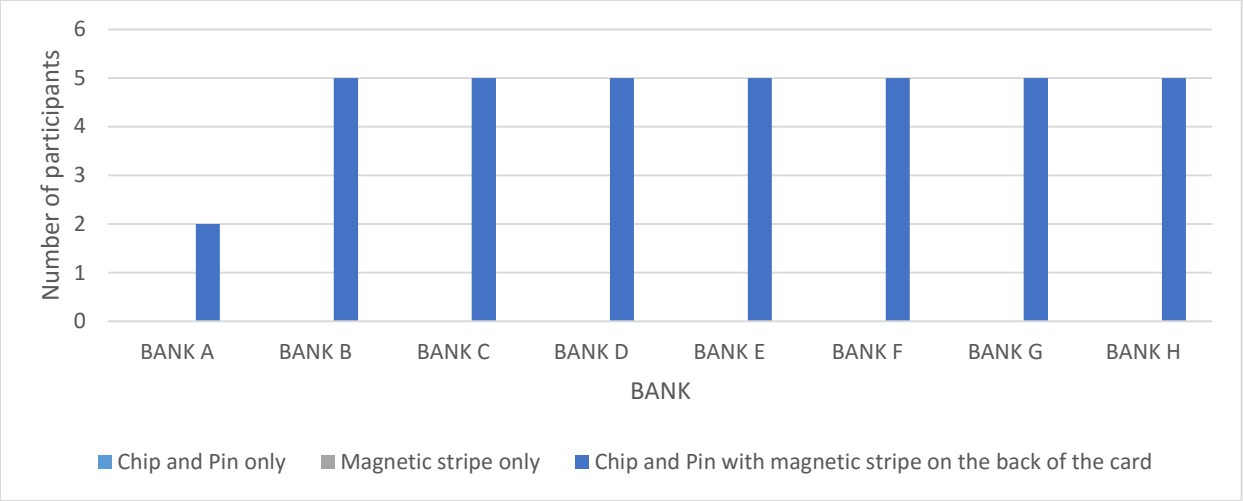

Figure 20: Banks Migration to EMV Chip and Pin Card

12) Period of Occurrence of ATM Fraud

From Figure 21, respondents from Bank C, Bank D and Bank H said that the ATM fraud occurred whilst the bank was still using magnetic stripe cards. Respondents from Bank E said the ATM fraud occurred after the migration to the EMV Chip and Pin card. 67% of the respondents from bank B said the fraud occurred whilst using the magnetic stripe card while 33% of the respondents said the fraud occurred after migrating to the EMV Chip and Pin card. 40% of the respondents from Bank F said the fraud occurred whilst using the magnetic stripe card while 60% of the respondents said the fraud occurred after migrating to the Chip and Pin card. 60% of the respondents said the fraud occurred whilst using the magnetic stripe card, while 40% of the

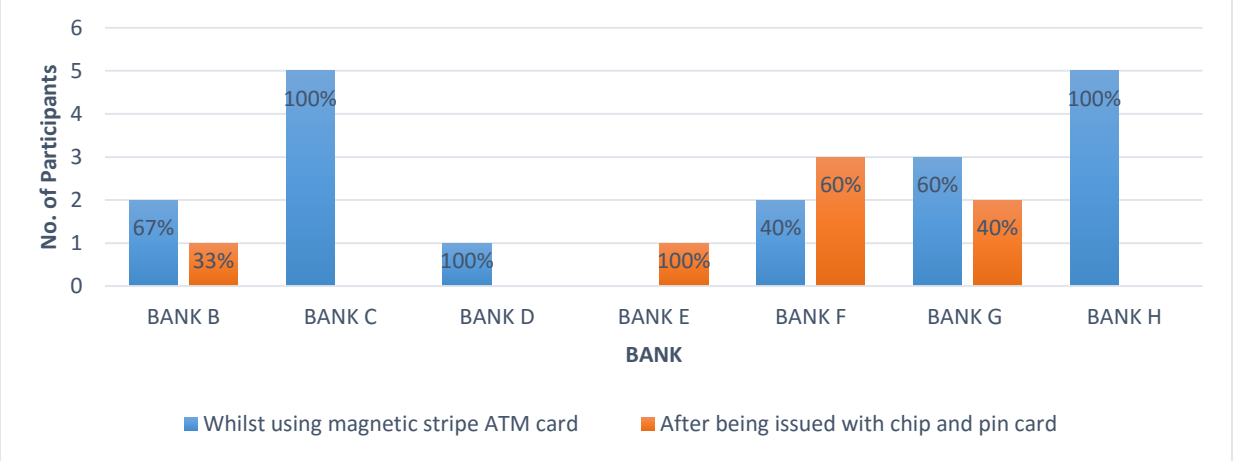

Figure 21: Period of Occurrence

respondents said the fraud occurred after migrating to the Chip and Pin card. This shows that ATM fraud still occurs even after the banks migrated to the EMV Chip and Pin card.

13) Sharing of ATM card and Pin

As can be seen from Figure 22, it can be seen that from the married respondents, 53.5% share both their ATM card and PIN with their spouse. 17.9% said their spouses have access to their ATM cards but don't know the PIN. 10.7% of the respondents said their spouses know their PIN but have no access to their ATM cards. Only 17.9% of the married respondents keep both their cards and their PIN from their spouses.

An ATM card is personal and ATM users should keep both their card and PIN safe.

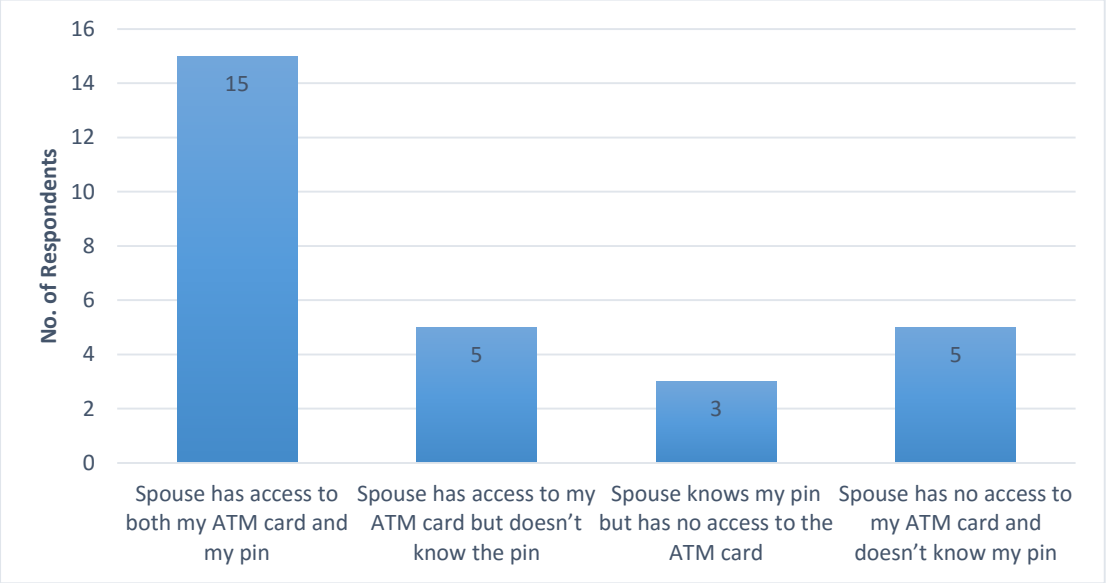

Figure 22: Sharing of ATM card and PIN

14) Securing of ATM Card PIN

From Figure 23, it can be seen that 86.5% memorize their ATM card PIN whilst 13.5% save their ATM card Pin on their phone. Saving a pin on the phone compromises the safety of an account as anyone who has access to the phone will have access to the Pin.

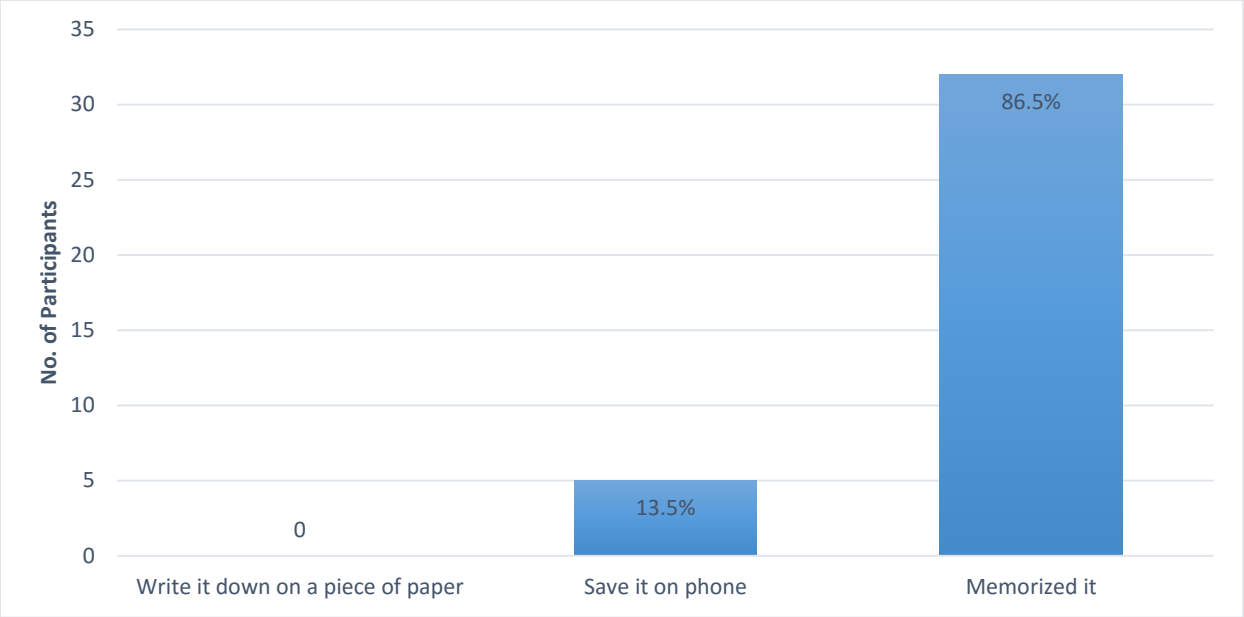

Figure 23: ATM Card PIN Safety

15) ATM Operating System

From Figure 24, it can be seen that banks have migrated their ATMs from windows XP operating system to windows 7 operating system. However, Bank C and Bank D still have some ATMs on windows XP. Windows XP is no longer supported and therefore no new patches are released for the vulnerabilities.

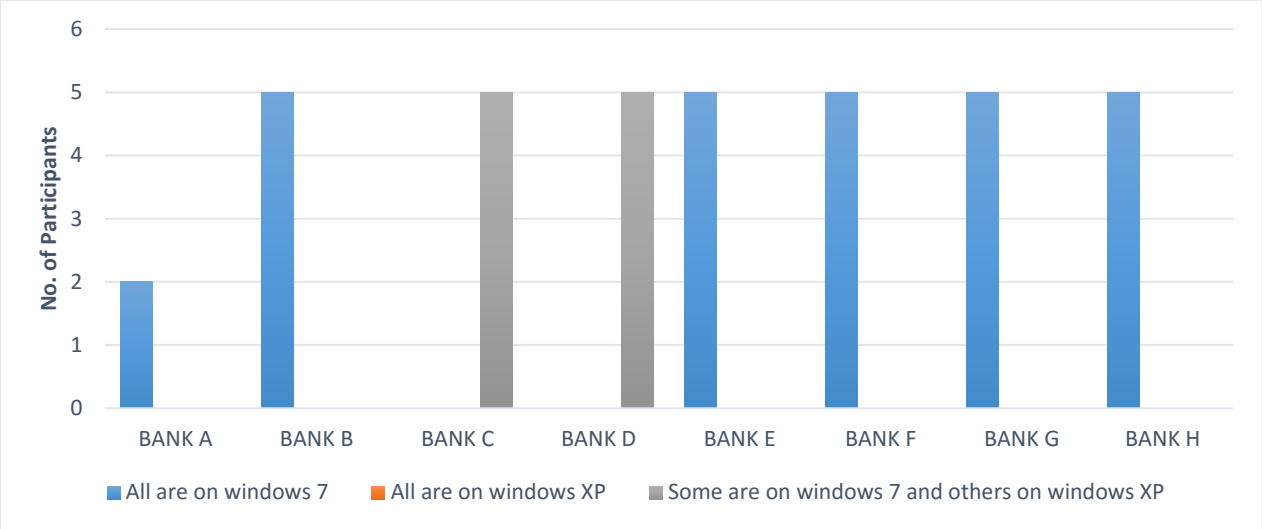

Figure 24: ATM Operating System

16) Firewall Configuration

From Figure 25, it can be seen that Bank E has no firewall configured. Bank A, Bank B, Bank C, Bank D, Bank F, Bank G and Bank H have a firewall configured on their network.

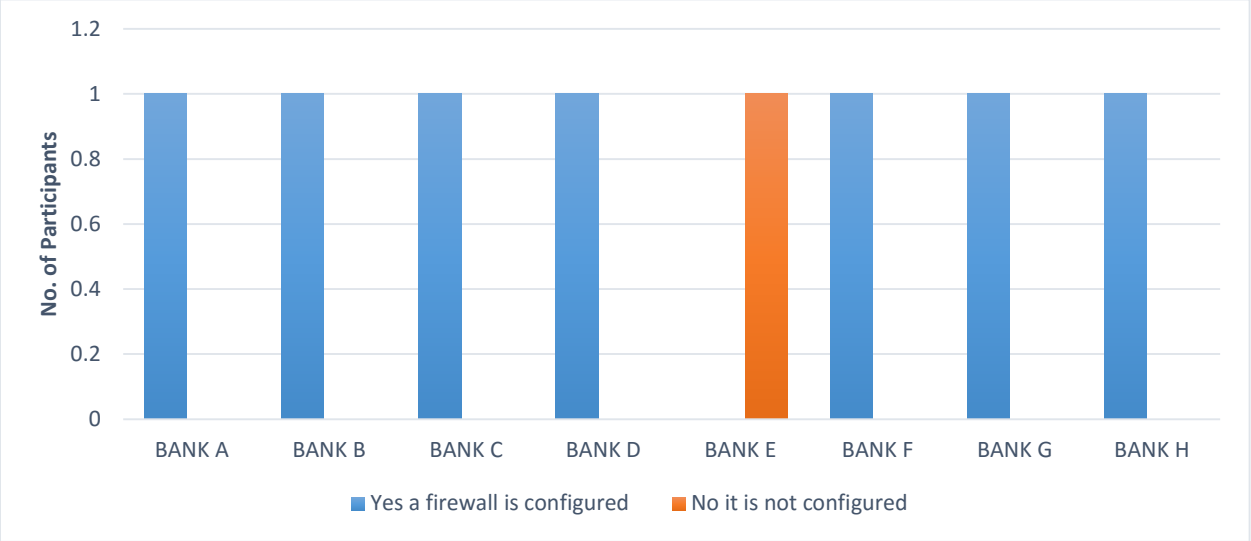

Figure 25: Firewall Configuration

17) ATM Login Password

From Figure 26, it can be seen that Bank A, Bank D, Bank E and Bank F still use vendor supplied passwords. Bank B, Bank C, Bank G and Bank H have changed their passwords from vendor supplied passwords to password created according to the banks password policy.

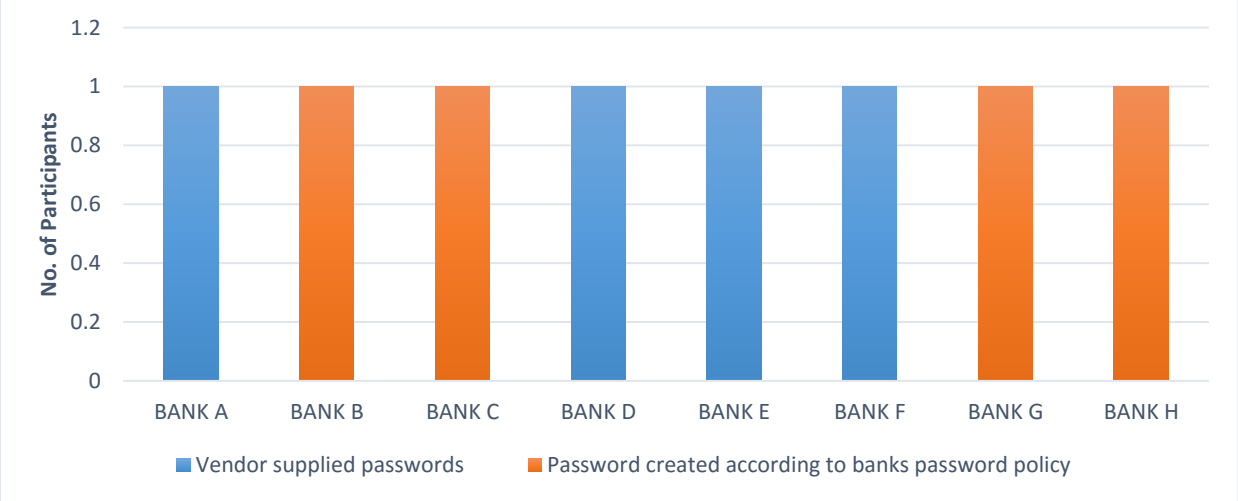

Figure 26: ATM Login Password

18) Card Holder Data Retention Policies

From Figure 27, Bank A, Bank B, Bank C, Bank D, Bank F, Bank G and Bank H have card holder data retention policies in place and the banks are using them. Bank E doesn't have any card holder data retention policy. The policy should give guidelines on how card holder data should be protected. PCI DSS demands that all companies that store card holder data should have card holder data retention policy in place.

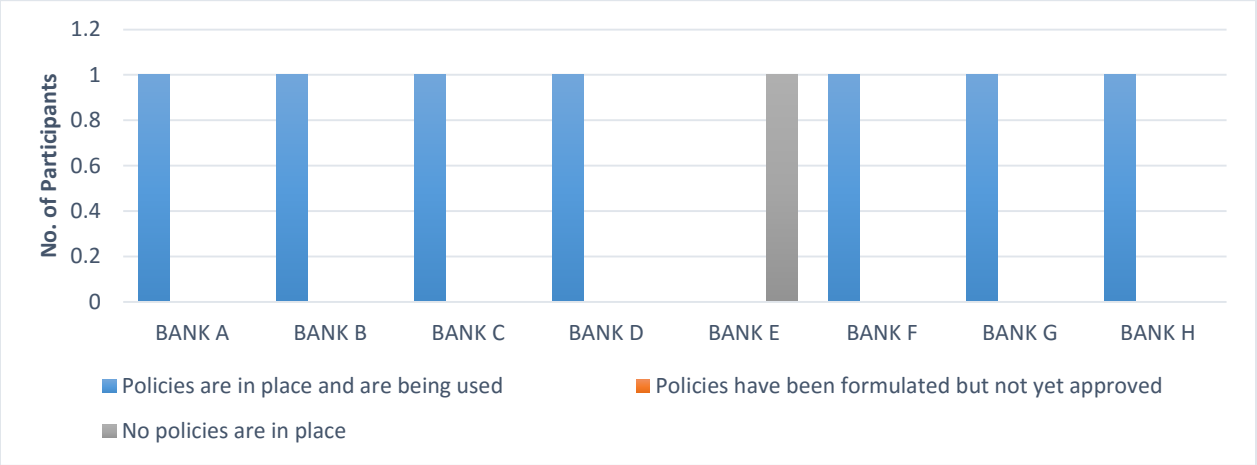

Figure 27: Card Holder Data Retention Policy

19) Encryption of Card holder data

From Figure 28, it can be seen that all the 8 banks encrypt card holder data.

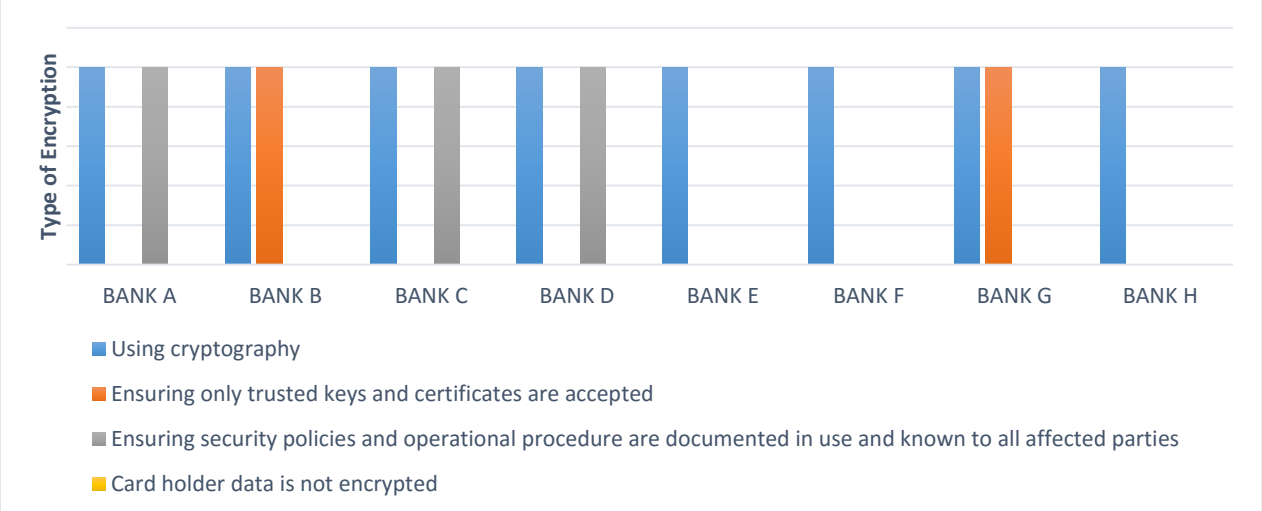

Figure 28: Encryption of Card Holder Data

Banks have no option on this PCI DSS requirement because an ATM can't work without loading encryption keys on the Encrypting Pin Pad(EPP). Bank A, Bank C and Bank D uses cryptography and ensures security policies and operational procedures are documented, in use and known to all affected parties. Bank B and Bank G uses cryptography and ensures only trusted keys and certificates are accepted. Bank E, Bank F and Bank H only use cryptography.

20) Responsibility of Loading Encryption Keys

From Figure 29, only Bank G and Bank H load their own encryption keys. Bank E totally depend on ATM vendors for the loading of encryption keys. Bank A, Bank B, Bank C, Bank D and Bank F uses both bank employees and vendors to load encryption keys. Giving vendors access to encryption keys compromises the security of card holder data as anyone who has access to them can get card holder data as long as they have the ability to intercept communication between the ATM and the ATM switch.

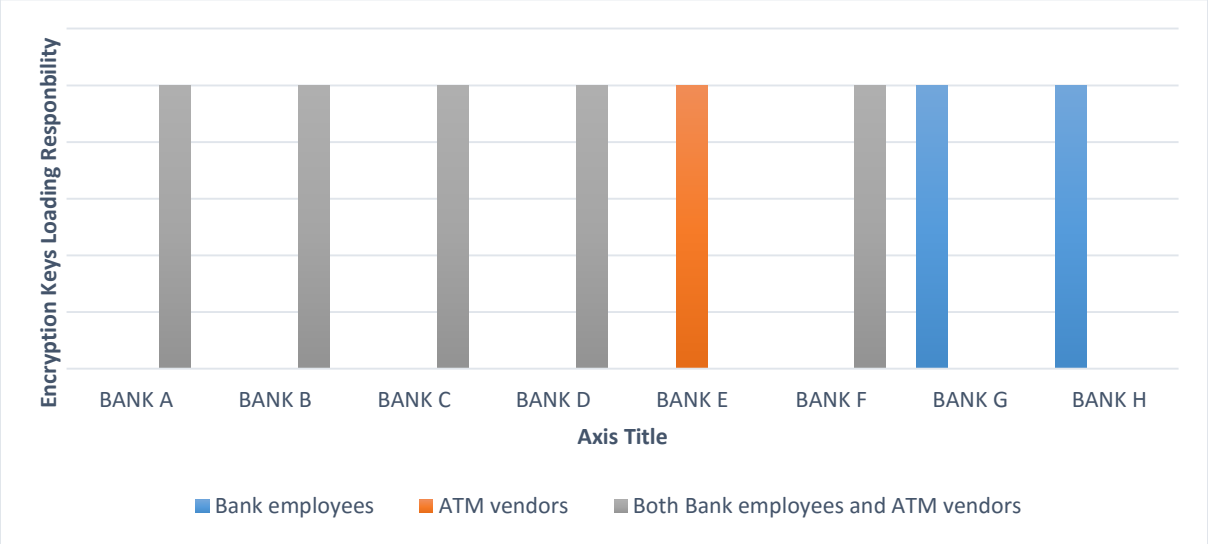

Figure 29: Loading of Encryption Keys

21) Anti-virus

From Figure 30 and Figure 31, Bank A and Bank G have an anti-virus installed on all the ATMs. Bank C, Bank E and Bank H has an anti-virus installed on some of the ATM and no anti-virus on some of the ATMs. Bank B, Bank D and Bank F have no anti-virus on all their ATMs.

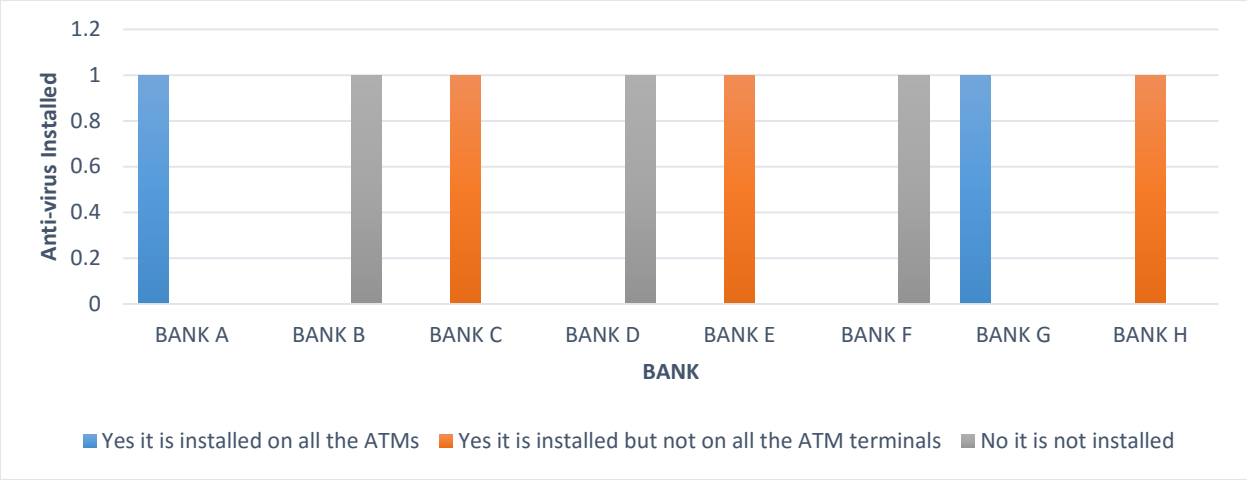

Figure 30: Anti-virus

22) Anti-virus update

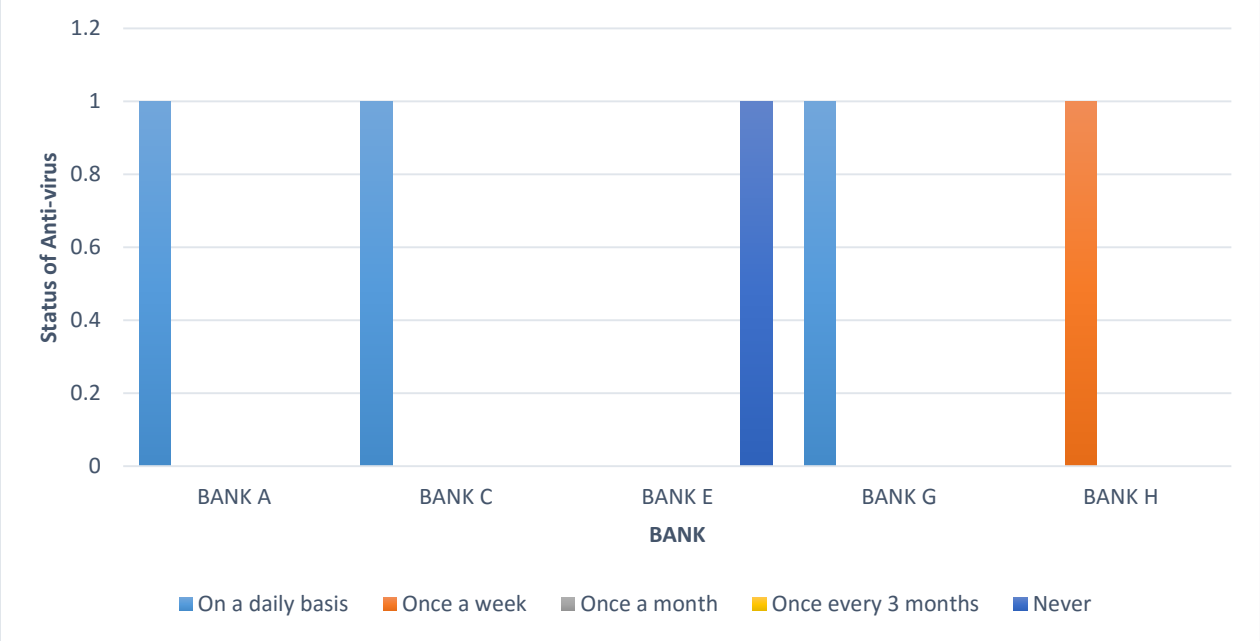

Figure 31: Anti-virus update

23) Vulnerability Scans

From Figure 32, Bank A, Bank B, Bank C, Bank D and Bank G carry out vulnerability scans once a month. Bank E, Bank F and Bank H never do vulnerability scans. Vulnerability scans are important as the banks can patch the vulnerabilities discovered before a hacker has a chance to exploit the vulnerability.

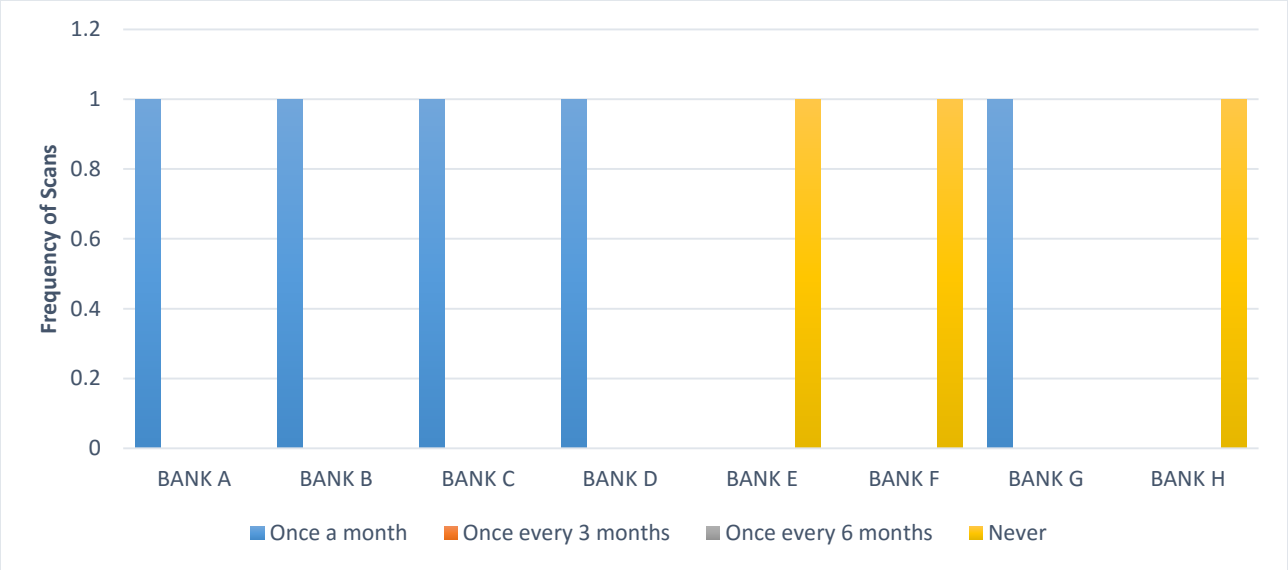

Figure 32: Scans

4.2.2 PCI DSS Compliance

In this section the statistics of the banks compliance to PCI DSS will be covered.

From Table 15 and Figure 33, it can be seen that Bank A is 75% compliant, Bank B and Bank G are 83% compliant, Bank C, Bank D, and Bank H are 58% compliant, Bank E is 50% compliant and Bank F is 67% compliant to the PCI DSS. The average level of compliance by the banks to the PCI DSS is 66.5%.

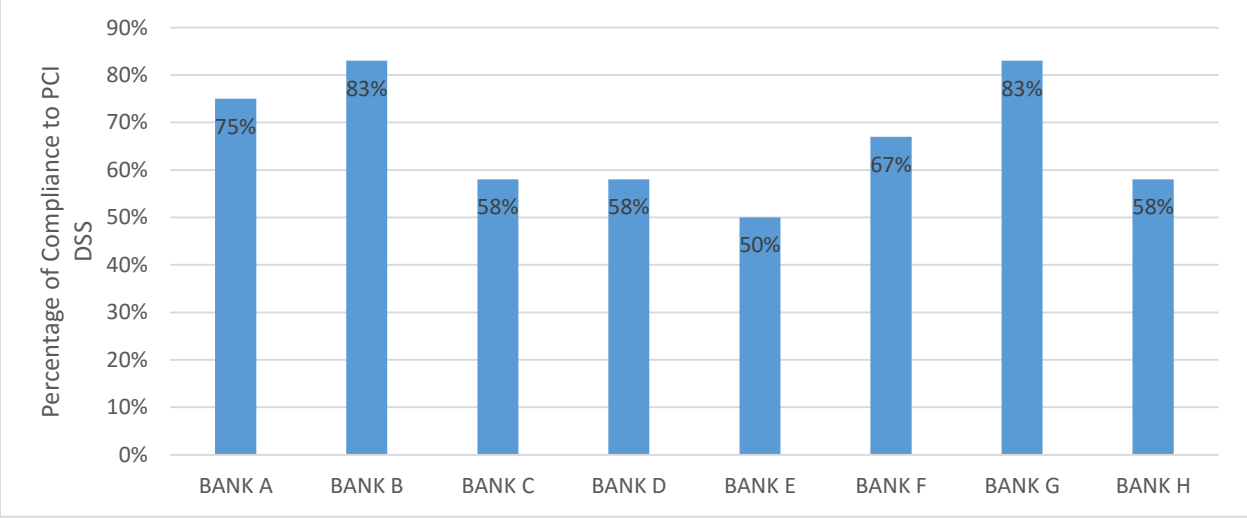

Figure 33: PCI DSS Compliance Percentage

Table 15: Banks PCI DSS Compliance

	PCI DSS Requirement	Bank A	Bank B	Bank C	Bank D	Bank E	Bank F	Bank G	Bank H	PCI DSS Requirement Compliance
1	Install and maintain a firewall configuration to protect data	√	√	√	√		√	√	√	88%
2	Do not use vendor-supplied defaults for system passwords and other security parameters		√	√				√	√	50%
3	Protect stored cardholder data	√	√		√	√	√	√	√	88%
4	Encrypt transmission of cardholder data across open, public networks	√	√	√	√	√	√	√	√	100%
5	Use and regularly update anti-virus software or programs	√						√		25%
6	Develop and maintain secure systems and applications	√	√			√	√	√	√	75%
7	Restrict access to cardholder data by business need-to-know	√	√		√	√	√	√		75%
8	Assign unique ID to each person with computer access									0%
9	Restrict physical access to cardholder data	√	√	√	√	√	√	√	√	100%
10	Track and monitor all access network resources and cardholder data		√	√	√		√			50%
11	Regularly test security systems and processes	√	√	√	√			√		63%
12	Maintain a policy that addresses information security for employees and contractors	√	√	√		√	√	√	√	88%
	BANK PCI DSS COMPLIANCE	75%	83%	58%	58%	50%	67%	83%	58%	

4.3 ATM Crime Statistics

In this section, the statistics obtained from BOZ on ATM crime when the banks were using the magnetic stripe card and after the migration to the EMV Chip and Pin card are presented. This was to determine if the introduction of the Chip and Pin card in Zambia has helped reduce ATM crime.

24) No. of Debit Card Issued

From Figures 34 and 35, it can be seen that the total number of ATM cards increased from 2,586,036 to 2,929,438 to 3,234,637 from 2015 to 2016 to 2017.

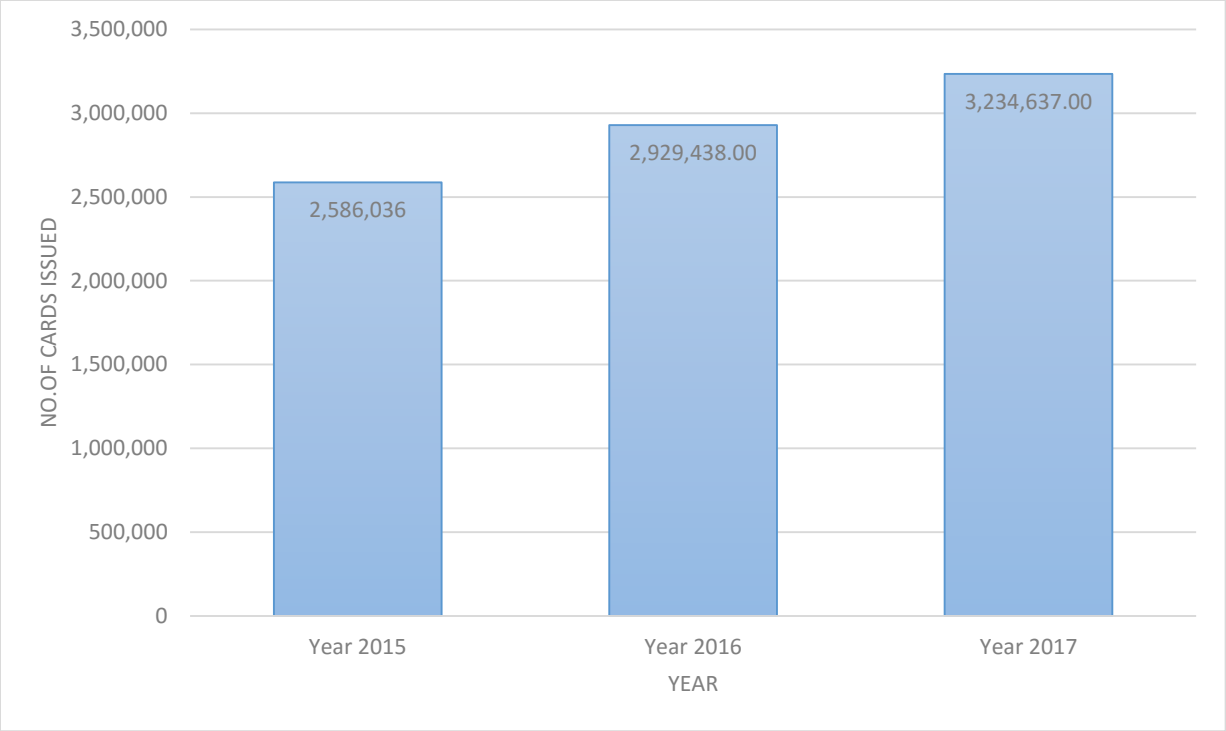

Figure 34: Debit Cards Issued

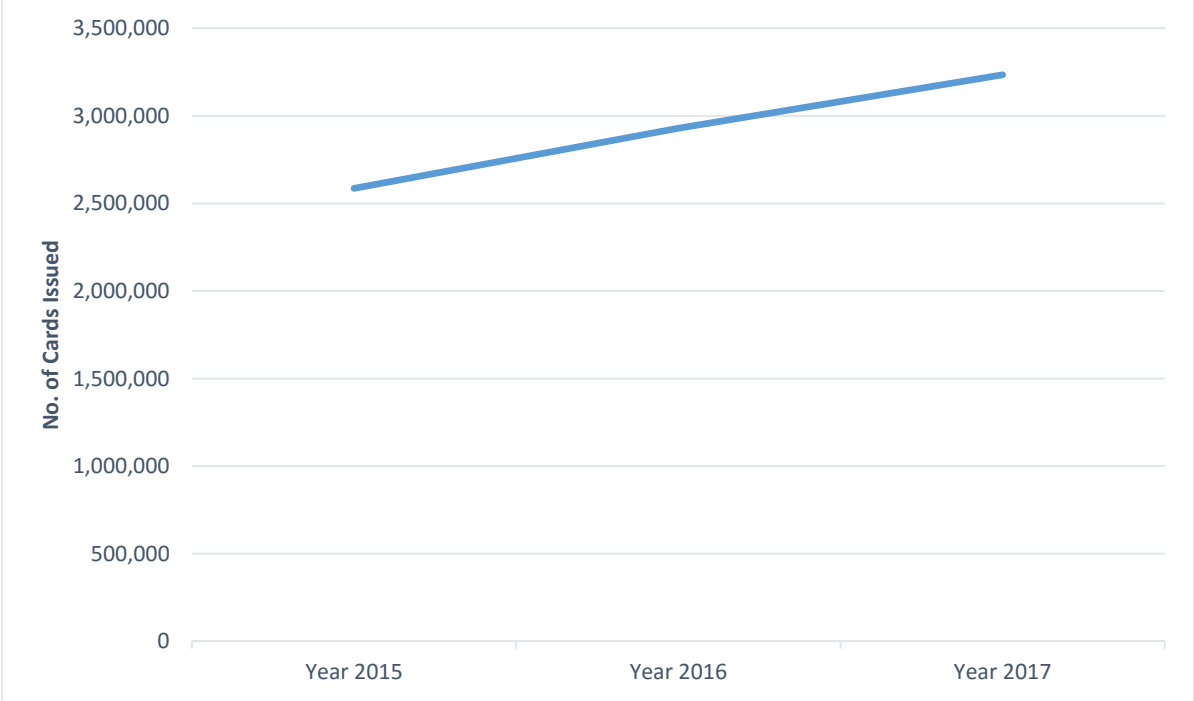

Figure 35: Trend of Issued Cards

25) Cards Compromised

From Figures 36 and 37, it can be seen that the number of cards compromised in Year 2015, when banks were issuing magnetic stripe cards was 289. In 2016, after the introduction of the Chip and Pin card, the number of cards that were compromised was 642. In 2017, the number of cards compromised increase to 782.

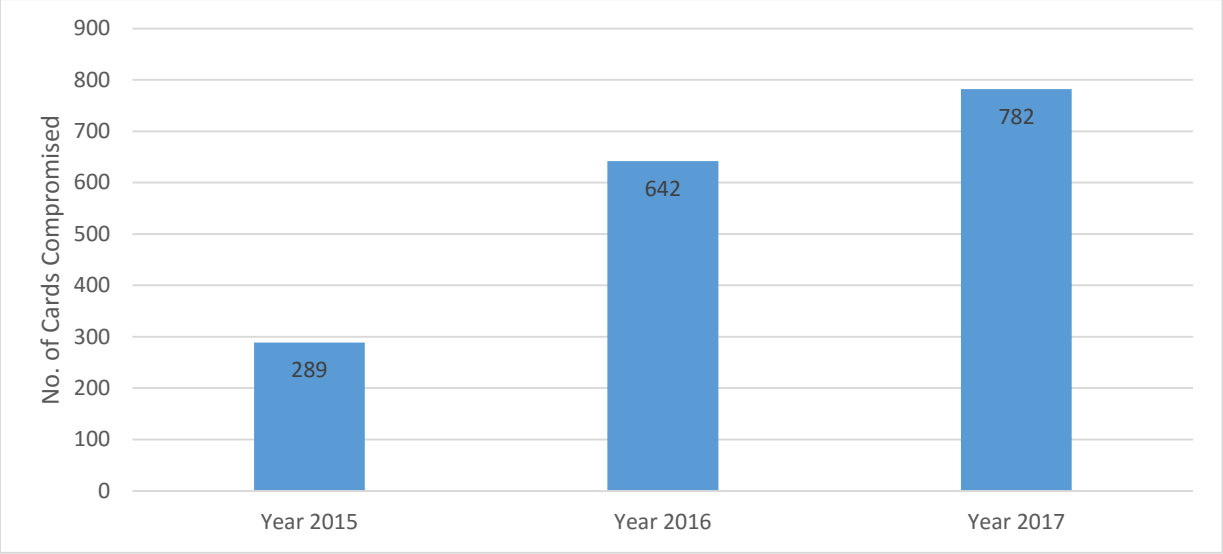

Figure 36: Cards Compromised

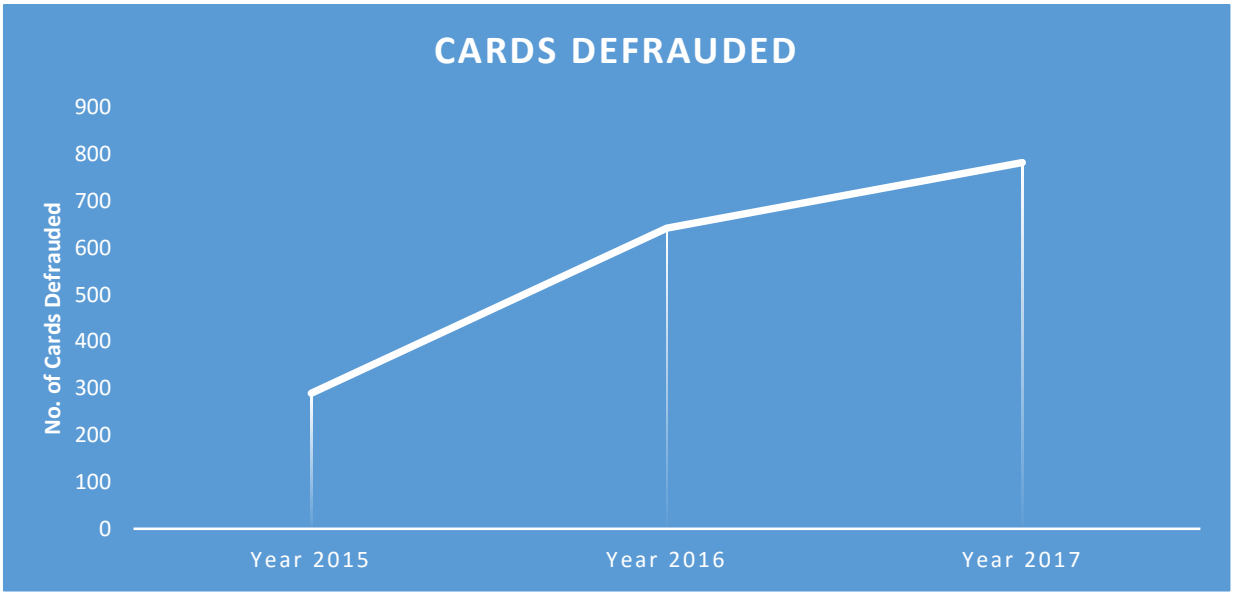

Figure 37: Trend of Cards Defrauded

26) Money Defrauded

From Figures 38 and 39, banks lost ZMK 2,444,960.00 due to ATM fraud in 2015. In 2016, banks lost ZMK 4,061,618.20 due to ATM fraud and in 2017, banks lost ZMK 9,172,446.90 due to ATM fraud. ATM fraud increased in 2016 and 2017 even after commercial banks introduced the EMV Chip and Pin card to help reduce ATM crime.

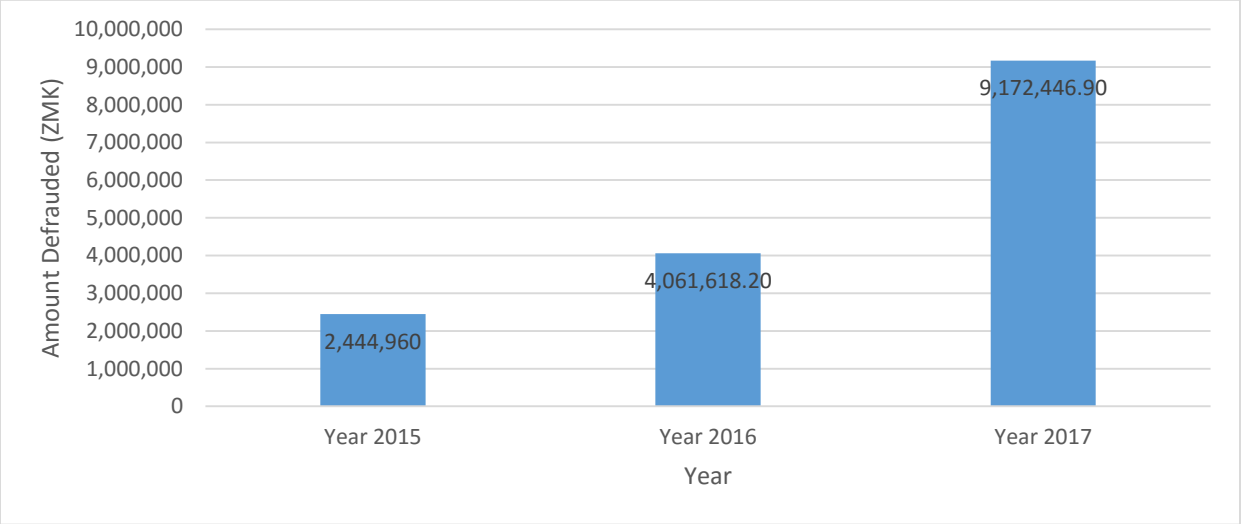

Figure 38: Money Defrauded

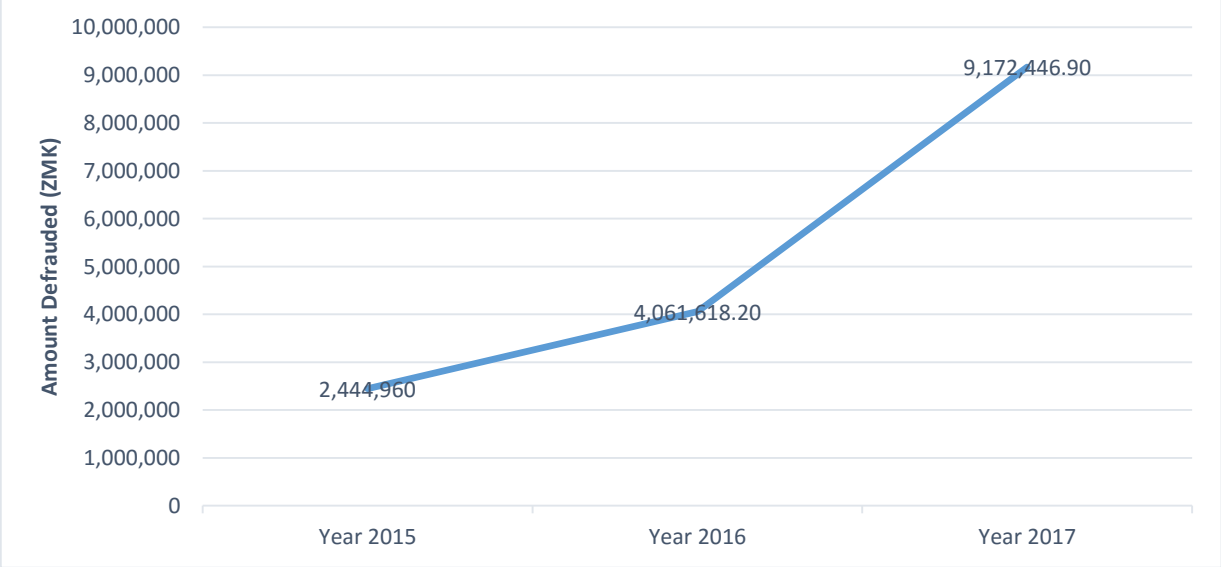

Figure 39: Trend of Money Defrauded

4.4 Proposed Conceptual ATM Security Framework

This section covers the proposed conceptual framework to help enhance ATM security based on the results obtained from the baseline study.

Figure 40, shows the proposed conceptual framework to help banks enhance ATM security in Zambia which is based on the results obtained from the baseline study. From the baseline study, it has been noted that human security is not adequately dealt with as can be noted that there is 100% non-compliance to PCI DSS requirement 8. It is a 6 layered framework supported by 2 pillars.

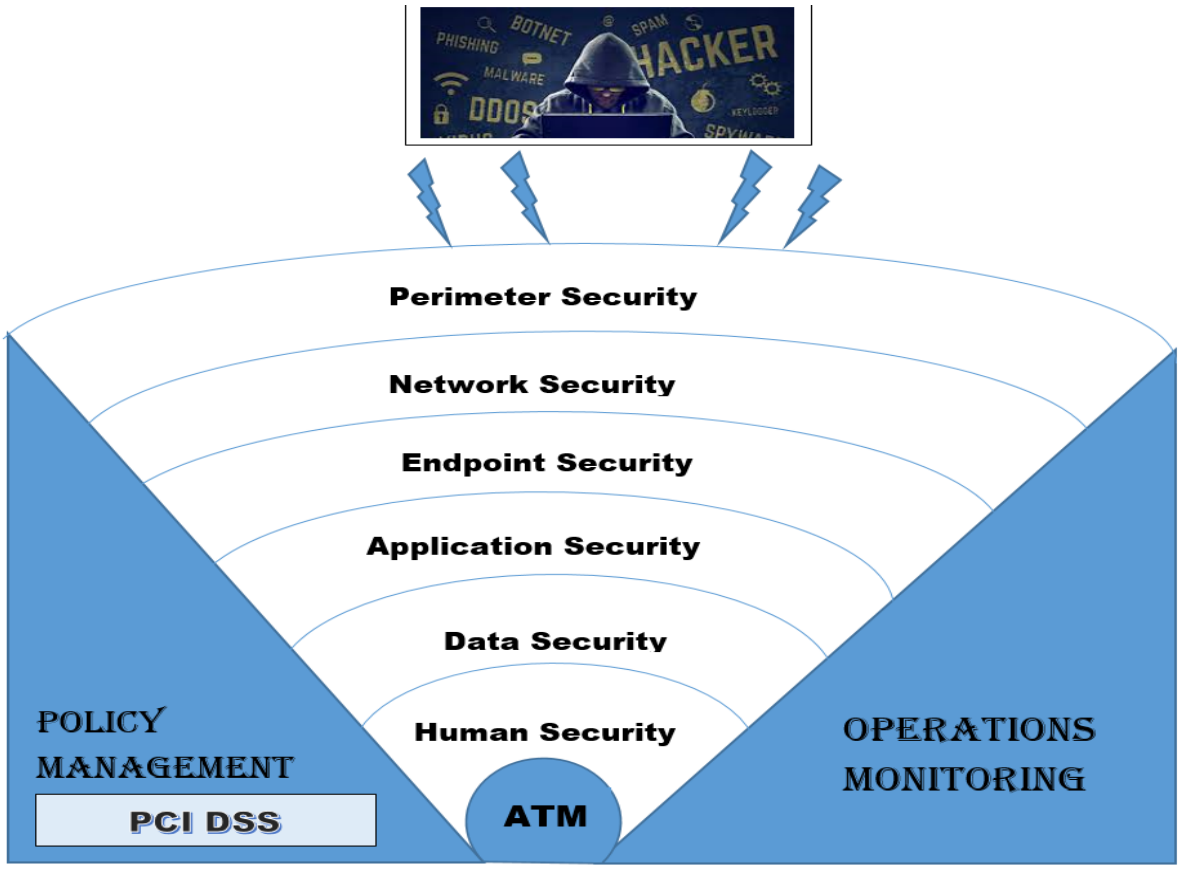

Figure 40: Proposed Conceptual ATM Security Framework

The framework offers security at 6 layers (human Security, data security, application security, endpoint security, network security and perimeter security. Different solutions are deployed at the different layers enhancing the security of the ATM. The multi-layers of security are supported by policy management pillar and operations monitoring pillar. The PCI DSS has been incorporated

in the framework and is part of the policy management pillar. This framework was adopted from the critical asset framework but the human security layer has been added. The 6 layers of the frameworks should have the following controls:

1) Perimeter Security

1. Perimeter Unified Threat Management (UTM) Firewall to offer multiple layer security, including next-generation firewalls, intrusion detection/prevention systems, antivirus, virtual private networks (VPN), spam filtering and URL filtering for web content,
2. Install Intrusion Detection and Prevention Systems (IDPS),
3. Install spam filter solution,
4. Install a Honey Pot to act as a decoy to lure cyber-criminals, and to detect, deflect or study attempts to gain unauthorized access to information systems,

2) Network Security

5. ATM network must be separated from the rest of the banks network by using firewalls and VLANs,
6. Implement network access control (NAC) that acts as an automated detection and response system to react to breaches and damage in real time,
7. Web proxy content filtering

3) Endpoint Security

8. Hard Disk Encryption,
9. Hard Disk Hardening,
10. Host IDS/IPS,
11. Implement Strong Password,
12. Do not use vendor supplied passwords,
13. Use Biometrics Authentication,
14. BIOS must be read only or Password protected,
15. Disable boot from external devices like CD, USB,
16. Use anti-malware and anti-virus software and regularly update them,
17. Control physical access to ATM rooms by ensuring the ATM has security doors, CCTV, motion detectors and intrusions Alarms is installed, and access logs are reviewed regularly.

4) Application Security

18. Patch Management,
19. Update ATM software regularly including firmware
20. Use supported operating system.
21. Web Application Firewall
22. Software whitelisting

5) Data Security

23. Encryption,
24. Public Key Infrastructure(PKI)
25. Data Loss Prevention(DLP)
26. Enterprise Right Management

6) Policy Management (Preventive)

1. Implement PCI DSS
2. ICT Security Policy,
3. Password policy must be in place,
4. Implement EMV chip and pin card and eliminate magnetic stripe fall back,
5. Define a detailed network topology and data flow diagrams that will help understand how the ATM is connected to the rest of the network and to the ATM switch; is it segregated, is it behind a firewall.
6. Implement an incidence response policy for ATM fraud and security incidences.
7. Implement processes to regularly inspect ATM physical components for any tampering
8. Conduct Vulnerability assessments
9. Conduct Penetration assessments
10. Conduct regular risk assessment: a risk assessment will help the bank know the security posture of the bank's critical assets including the ATM and will help them determine the following; How the ATMs are connected to the network, what physical and logical security measures are in place, and the people with access to the ATM (Employees, ATM vendors, and other service personnel). Conduct third party risk assessments to identify third party risk.

7) Operations Management

11. Digital Forensics

12. Install transaction level real time monitoring system,
13. Install a privileged user management system to monitor and alert when system configuration changes,
14. Implement a SIEM: SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The software then identifies and categorizes incidents and events, as well as analyzes them. The software delivers on two main objectives, which are to:
    i. provide reports on security-related incidents and events, such as successful and failed logins, malware activity and other possible malicious activities and
    ii. send alerts if analysis shows that an activity runs against predetermined rulesets and thus indicates a potential security issue.
    iii. Auditors use it to check for compliances
    iv. New SEIM software have threat intelligence
15. Build a Security Operations Center (SOC): A security operations center is a center used for continuously monitoring and managing the security status of an organization. Its aims at enhancing incident detection, investigation, and response capabilities using data from endpoint devices, logs, security systems, and network flows. An effective SOC can help organizations build robust situational awareness and prioritize the deployment of enterprise resources to address security issues.

4.5 Chapter Summary

The chapter presented the results of the baseline study and the ATM fraud statistics from Bank of Zambia. It also presented the proposed framework that commercial banks can use to enhance ATM security.

CHAPTER FIVE: DISCUSSION AND CONCLUSION

5.1 Chapter Introduction

From the discussion in Chapter 4, the following are some of the recommendations that were deduced from the data that was gathered. The chapter begins with the discussion of the findings of the research and then gives the conclusion based on the findings and discussion given. It then gives the recommendations and looks at the possible future works that can be done pertaining to the research. Part of the findings of this research were published in the International Journal of Advanced Studies in Computer Science and Engineering Volume 7, Issue 10 (IJASCSE).

5.2 Discussion

This section discusses the implementation and results that were implemented in the previous chapter and how they relate to the objectives and research questions of this study.

As a way to justify the proposal of a framework to help enhance ATM crime, statistics on ATM crime before and after the introduction of the EMV Chip and Pin ATM card were obtained from Bank of Zambia. This was to determine if the introduction of the new card has helped Zambia mitigate ATM crime. Questions based on the PCI DSS were also asked to the 8 participating commercial banks to determine their level of compliance to the PCI DSS.

5.2.1 The Baseline Study

The first objective sought to investigate the level of ATM security in Zambia based on PCI DSS. The study revealed that commercial banks in Zambia are not 100% to the PCI DSS. The most compliant banks, Bank B and Bank G are 83% compliant. The least compliant Bank, Bank E is 50% compliant. The average compliance level for the 8 banks is 66.5%. The research showed that commercial banks are not benefiting from the implementation of PCI DSS, because the benefits of implementing can only be realised by being 100% compliant. The results also revealed that the banks don’t consider protecting card holder data as a priority as some banks don’t even have the most common security control; anti-virus. Only Bank A and Bank G have an anti-virus installed on all their ATMs. Some Banks have an anti-virus on some of their ATMs while other ATMs don’t have. This is as good as not installing on all of them as malware on an ATM without an anti-virus can easily propagate to the whole ATM network. It is very risky to have ATMs without an anti-

virus as the Jackpotting attack discussed in chapter 2, uses malware as one of the ways it gets on the ATM. Without an anti-virus on some of the ATMs, Zambia is at risk of being hit by this new ATM attack which hit the USA in 2018 and banks lost US$1 million. Bank A, Bank D, Bank E, Bank F use vendor supplied passwords to log onto the ATM, giving access to the vendors. This is a vulnerability on the ATM as even the individuals that once worked with the vendors know the default ATM password. The recommendation by PCI DSS is that all the default passwords should be changed in order to protect card holder data. None of the banks is compliant with requirement 8, which is to assign a unique ID to each person with computer access. The ATM only has one login credential even for the ones that have changed the default password. It is therefore to achieve the information security objective of accountability as long as the person that logged into the ATM used the correct password.

5.2.2 ATM Crime Statistics

The second objective was to determine if the introduction of the EMV chip and pin card has helped reduce ATM crime in Zambia. The chip and pin card was introduced in 2015. As it can be seen from the results, the total number of debit cards that were issued by the commercial banks increased by 13.3% from 2015 to 2016. The number of debit cards issued further increased by 10.4% in 2017. Increasing the number of debit cards, increases the number of transactions on the ATM and also increases the change of debit cards being compromised. The number of debit cards compromised increased by 122.10% from 2015 to 2016 as can be seen from the results. The number further increased by 21.8% in 2017. An increase of 122.1% is large and commercial banks should ensure that measures to protect card holder data are all in place. This goes back to the fact that banks should comply 100% to the PCI DSS in order to mitigate this card fraud. The increase in the number of cards compromised could also be due to the increase in the debit cards issued. In monetary terms, the amount of money banks lost increased by 66.1% from 2015 to 2016. The amount further increased by 125.8% in 2017. The amount of money defrauded is indirectly proportional to the number of cards defrauded as can be seen from the results. The amount of money defrauded depends on the amount of money the card holders whose cards have been defrauded have in their accounts. The amount of money defrauded would increase if the banks experience the new ATM attack; jackpotting which doesn't only target one ATM card but targets the money in the ATM.

5.2.3 Proposed ATM Security Framework

The third objective which was to propose a framework to help enhance ATM security. We adopted a framework for the protection of critical assets. An ATM is considered a critical asset as all the participants in the research feel the ATM has improved the way banking is done. An ATM is used to withdraw money from people's accounts and compromising an ATM compromises peoples accounts and also the banks money. An ATM is also connected to the banks switch which is connected to the core banking system; and compromising the ATM can compromise the core banking system. The multi-layered framework that protects mission critical assets was adopted and an extra layer of security which is human security was added to the framework. A multi-layered framework was proposed as even the best available information assurance products have inherent weaknesses which with time can be exploited. A countermeasure is to deploy a multiple defence mechanism to protect the ATM. A security solution is as good as the weakest link, which is the human element in ICT security. The framework proposed hopes to achieve information assurance using a balanced focus on three primary elements: People, Technology and Operations;

People: In order to achieve Information assurance, it begins with senior management who should understand the perceived threat. Policies and procedures must be defined, and role and responsibilities must also be assigned. Critical personnel must also be trained in the deployed security technologies and also in personal accountability. The people element is covered in the framework by the Human security layer.

Technology: Many technologies that provide information assurance services and detect intrusions are available today. The banks should establish effective policy and processes for technology acquisition. This will help the banks defend the networks and infrastructure and also defend the enclave boundaries. The technology element is covered by Perimeter security layer, Network security layer, Endpoint security layer, Application security layer and Data security layer.

Operations: The operations element is covered by the 2 supporting pillars Policy Management and Operations Monitoring. This focuses on all the activities that an organisation requires to sustain its security posture on a day to day basis.

5.2.5 Comparison with Other Similar Works

As has been covered in Chapter 1, significant work in the area of ATM security has been done by many researchers. However, the works that have been done in the past focused on ATM crime that compromise authentication. This research proposed a framework that helps the ATM achieve all the security objectives of confidentiality, integrity, availability, authentication, authorisation and privacy.

5.2.6 Possible Application

The work in this study is an attempt to help reduce ATM crime in Zambia. The commercial banks can adopt this multi-layered framework and deploying different technologies to help them protect the ATM. This framework can also be adopted when protecting any other critical asset in order to ensure information assurance.

5.3 Summary

This study proposed a multi-layered framework that banks in Zambia can use to enhance ATM security. This framework will help the country mitigate the existing ATM fraud and will help the country to be cyber-ready for emerging ATM crimes like Jackpotting and ATM Shimming attack. This framework is easy to implement as it is multi-layered. It is also easy for a bank to see which layer hasn't been protected. The human element who is the weakest link in cyber security has also been taken care of. Commercial banks should ensure a security solution is implemented at each layer to ensure all the proposed 5 layers are secured. The 2 supporting pillars must also be functional and the banks should ensure they are 100% with PCI DSS in order to realise its full benefits.

5.4 Conclusion

Commercial banks in Zambia can reduce ATM fraud by being 100% compliant to PCI DSS. The security measures that have been implemented by commercial banks in Zambia to protect ATMs are not adequate. The banks can enhance ATM security by using the proposed ATM security framework which is a 6 layered framework and includes Human security. The framework also recommends ATM software whitelisting to mitigate against ATM Jackpotting attack.

5.5 Future Works

This research proposed a conceptual framework to enhance ATM security in Zambia but did not include online card transaction fraud amongst Zambians. A research can also be done to determine if the deployment of biometrics on ATMs in Zambia can be appreciated.

REFERENCES

[1] K. Hooda, "ATM Security," *International Journal of Scientific and Research Publications,* vol. 6, no. 4, 2016.

[2] A. Taha , A. Morteza and G. Zeinab , "SFAMSS: A SECURE FRAMEWORK FOR ATM MACHINES VIA SECRET SHARING".

[3] K. Tuli and G. Kaur, "ATM SAFETY & SECURITY," *International Journal of Advanced Research in,* vol. 2, no. 2, 2013.

[4] N. K. Gyamfi and N. Y. Asabere, "Towards Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective," *International Journal of ICT and Management,* vol. 1, no. 2, 2013.

[5] N. K. Gyamfi, M. A. Mohammed, K. Nuamah-Gyambra, F. Katsriku and J.-D. Abdulah, "Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective," *International Journal of Applied Science and Technology,* vol. 6, no. 1, 2016.

[6] K. Namusa, "Zambia: Cyber Crime Costs Banks U.S.$4 Million," Allafrica, 14 June 2013. [Online]. Available: http://allafrica.com/stories/201306141287.html. [Accessed 28 February 2018].

[7] J. Bloomberg, "ATM 'Jackpotting' Attacks Reveal Deeper Problems," 12 02 2018. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2018/02/12/atm-jackpotting-attacks-reveal-deeper-problems/#5b1147ee6fc3. [Accessed 10 04 2018].

[8] M. O. Onyesolu and I. M. Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study," *International Journal of Advanced Computer Science and Applications,* vol. 3, no. 4, 2012.

[9] J. Wellington, "Reviewing the Research Literature," in *Educational Research: Contemporary Issues and Practical Approaches*, London, Bloomsbury, 2015, pp. 55-80.

[10] Reuters, “World's first ATM Machine turns to gold on 50th birthday,” Reuters, 27 June 2017. [Online]. Available: https://www.reuters.com/article/us-atm-anniversary/worlds-first-atm-machine. [Accessed 08 November 2018].

[11] S. Verma, “Invention Story of ATM,” [Online]. Available: https://www.engineersgarage.com/invention-stories/atm-history. [Accessed 7 December 2018].

[12] J. M. Stewart, M. Chapple and D. Gibson, Certified Information Systems Security Professional, New Delhi: Jim Minatel, 2015.

[13] Cybrary, “Authentication,” Cybrary, [Online]. Available: https://www.cybrary.it/glossary/a-the-glossary/authentication/. [Accessed 3 December 2018].

[14] J. M. Stewart, M. Chapple and D. Gibson, “Managing Identity and Authentication,” in *Certified Information Systems Security Professional*, New Delhi, Wiley India Pvt. Ltd, 2015, pp. 555-592.

[15] S. Choi and D. Zage, “Addressing Insider Threat using “Where You Are” as Fourth Factor Authentication,” in *2012 IEEE International Carnahan Conference on Security Technology*, Boston, 2012.

[16] P. Hames, “Solidcore Overview,” 17 08 2010. [Online]. Available: https://ncr.csod.com/LMS/UserTranscript/OnlineClassView.aspx?qs. [Accessed 10 04 2018].

[17] M. Rouse, “Card Verification Value,” Search Financial Security, [Online]. Available: https://searchfinancialsecurity.techtarget.com/definition/card-verification-value. [Accessed 1 January 2019].

[18] “Chip Card Security: Why is EMV More Secure,” [Online]. Available: https://squareup.com/townsquare/why-are-chip-cards-more-secure-than-magnetic-stripe-cards. [Accessed 2 January 2019].

[19] “Malware,” Norton, [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html. [Accessed 06 September 2018].

[20] J. M. Stewart, M. Chapple and D. Gibson, “Malicious code and Application Attacks,” in *Certified Information Systems Security Proffesional*, New Delhi, Jim Minatel, 2017, pp. 880-892.

[21] R. R. Patel and C. S. Thaker, “Zero-Day Attack Signatures Detection Using Honeypot,” *International Journal of Computer Applications,* 2011.

[22] c. Cowan , F. Wagle , C. Pu and S. Beattie , “Buffer overflows: attacks and defenses for the vulnerability of the decade,” in *DARPA Information Survivability Conference and Exposition*, Hilton Head, 2002.

[23] Q. Zeng, M. Zhao and P. Liu, “HeapTherapy: An Efficient End-to-End Solution against Heap Buffer Overflows,” in *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Rio de Janeiro, 2015.

[24] A. Jalal and M. A. Zeb, “Security Enhancement for E-Learning Portal,” *International Journal of Computer Science and Network Security,* vol. 8, no. 3, 2008.

[25] R. Riley, X. Jiang and D. Xu, “An Architectural Approach to Preventing Code Injection Attacks,” *IEEE Transactions on Dependable and Secure Computing,* vol. 7, no. 4, pp. 351-365, 2010.

[26] E. Athanasopoulos, V. Pappas and E. P. Markatos, “Code-injection attacks in browsers supporting policies,” in *2nd Workshop on Web 2.0 Security & Privacy (W2SP)*, 2009.

[27] M. Martin and M. S. Lam, “Automatic generation of XSS and SQL injection attacks with goal-directed model checking,” in *SS'08 Proceedings of the 17th conference on Security symposium*, California, 2008.

[28] O. Wild, “Warning og Logical (Jackpot) Attacks on ATMs in the United States,” 26 January 2018. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/unsorted/jackpot_attacks_in_the_us_-_january_2018.pdf. [Accessed 16 November 2018].

[29] O. Wild, “Black Box attacks on ATMs in Germany,” 18 April 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR-Security-Alert-2016-04-Black-Box-Attacks-in-Germany.pdf. [Accessed 13 November 2018].

[30] O. Wild, “Black Box attacks on ATMs in Italy.,” 14 April 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR-Security-Alert-2016-03-Black-Box-Attacks-in-Italy.pdf. [Accessed 13 November 2018].

[31] O. Wild, “Personas Black Box attacks continue to grow in Europe, now reported in UK,” 18 August 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/ncr_security_alert_-_2016-11_expansion_of_black_box_attacks_to_the_uk.pdf. [Accessed 13 November 2018].

[32] B. Williams and A. Chuvakin, PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, Massachusetts: Syngress Publishing, 2011.

[33] A. B. Association, Data Security Handbook, Chicago: ABA Publishing, 2008.

[34] O. Bakay, V. Dudykevych and Y. Lakh, “Investigations of Payment Cards Systems Information Security Control,” in *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, 2013.

[35] A. Bhargav, PCI Compliance: The Definitive Guide, CRC Press, 2014.

[36] C. Blackwell, “The Management of Online Credit Card Data using Payment Card Industry Data Security Standard,” in *2008 Third International Conference on Digital Information Management*, London, 2008.

[37] PCI Security Standards Council, “Requirements and Security Assessment Procedures,” 2013. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf. [Accessed 05 December 2018].

[38] B. Williams and A. Chuvakin, PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, Massachusetts: Syngress Publishing, 2014.

[39] M. R. Shihab and F. Misdianti, “Moving towards PCI DSS 3.0 Compliance: A Case Study of Credit Card Data Security Audit in an Online Payment Company,” in *International Conference on Advanced Computer Science and Information Systems*, Jakarta, 2014.

[40] M. Kedgley, “PCI DSS Version 3.0: New Standard But Same Problems?,” EzineArticles, 30 October 2013. [Online]. Available: https://ezinearticles.com/?PCI-DSS-Version-3.0:-New-Standard-But-Same-Problems?&id=8093847. [Accessed 05 December 2018].

[41] Ş. Bahtiyar, G. Gür and . L. Altay, “ Security Assessment of Payment Systems under PCI DSS,” in *International Information Security Conference (SEC)*, 2014.

[42] R. Kidd, “Counting the cost of non-compliance with PCI DSS,” *Computer Fraud & Security*, vol. 11, no. 6, pp. 13-14, 2008.

[43] P. Douthit and K. Huang, “ST&E Is the Most Cost Effective Measure for Comply with Payment Card Industry (PCI) Data Security Standard,” in *Financial Cryptography and Data Security*, Berlin, Springer, 2008, pp. 321-322.

[44] TrustWave, “Trustwave Global Report,” 2014. [Online]. Available: https://www.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf. [Accessed 05 December 2018].

[45] Verizon, “Verizon Annual Report,” 2013. [Online]. Available: http://www.verizon.com/about/sites/default/files/2013_vz_annual+report.pdf. [Accessed 05 December 2018].

[46] Ponemon, “Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis.,” 2014. [Online]. Available: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis. [Accessed 06 December 2018].

[47] R. Morgan and R. Boardman, Data Protection Strategy: Implementing Data Protection Compliance, Andover: Sweet & Maxwell, 2012.

[48] R. J. Sullivan, “The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud,” 2013. [Online]. Available: https://www.kansascityfed.org/publicat/econrev/pdf/13q1Sullivan.pdf. [Accessed 06 December 2018].

[49] I. O. f. Standardization, “Standards,” International Organization for Standardization, [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed 18 December 2018].

[50] Certification Europe, “Information Security,” Certification Europe, [Online]. Available: https://www.certificationeurope.com/certification/iso-27001-information-security/. [Accessed 18 December 2018].

[51] T. Mataracioglu, “Comparison of PCI DSS and ISO/IEC 27001 Standards,” *ISACA,* vol. 1, pp. 1-5, 2016.

[52] IT Governance, “Information Security and ISO27001 – An Introduction,” 2006. [Online]. Available: http://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf. [Accessed 18 December 2018].

[53] Z. Lovric, “Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard,” in *Central European Conference on Information and Inteelligent Systems,* Varazdin, 2012.

[54] S. K. White and L. Greiner, “What is ITIL? Your guide to the IT Infrastructure Library,” CIO, 15 August 2017. [Online]. Available: https://www.cio.com/article/2439501/itil/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html. [Accessed 3 January 2019].

[55] S. M. Ali, T. R. Soomro and M. N. Brohi, “Mapping Information Technology Infrastructure Library with other Information Technology Standars and Best practices,” *Journal of Computer Science,* vol. 9, no. 9, pp. 1190-1196, 2013.

[56] S. Beissel, “Supporting PCI DSS 3.0 Compliance With COBIT 5,” *COBIT Focus,* vol. 1, pp. 1-7, 2014.

[57] A. Alfantookh, *An Approach for the Assessment of the Application of ISO 27001 Essential Information Security Controls.,* King Saud University, 2009.

[58] C. Southern, “7 Layers of Data Security: Mission-Critical Assets,” 14 June 2016. [Online]. Available: http://blog.cspire.com/7-layers-of-data-security-mission-critical-assets. [Accessed 7 January 2019].

[59] B. Jones, “Global Information Assurance Certification Paper,” 4 January 2005. [Online]. Available: https://www.giac.org/paper/gsec/4235/overview-dod-defense-in-depth-strategy/106802. [Accessed 9 January 2019].

[60] M. Nicho, “Effectiveness of the PCI DSS 2.0 on Preventing Security Breaches: A Holistic perspective,” International Journal of Information Security and Privacy, USA, 2011.

[61] M. Haran and N. McKelvey, “PCI Compliance - No excuses, please,” *International Journal of Information & Security* , vol. 2, no. 2, pp. 118-123, 2012.

[62] R. J. Sullivan, “The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options,” 2010. [Online]. Available: www.KansasCityFed.org. [Accessed 07 July 2018].

[63] M. Nicho, “Incorporating COBIT Best Practices in PCI DSS V2.0 for Effective Compliance,” *ISACA Journal,* vol. 1, no. ISACA, 2012.

[64] J. Hizver and T.-c. Chiueh, “Automated Discovery of Credit Card Flow for PCI DSS Compliance,” in *30th IEEE International Symposium on Reliable Distributed Systems*, Stony Brook, 2011.

[65] H. Susanto, M. N. Almunawar and Y. C. Tuan, “Information Security Management System Standards: A Comparative Study of the Big Five,” *International Journal of Electrical & Computer Sciences* , vol. 11, no. 5, 2011.

[66] K. Berezina, “Top issues in PCI DSS compliance in hotels: an explaratort study,” *Journal of Hospitality and Tourism Technology,* vol. 1, no. 3, 2010.

[67] M. Karovaliya, S. Karedia, S. Ozac and D. R. Kalbande, “Enhanced security for ATM machine with OTP and Facial recognition features,” in *International Conference on Advanced Computing Technologies and Applications (ICACTA-2015),* Mumbai, 2015.

[68] P. Jindal and R. Kumar, “Analysis of Security System for ATM,” in *4th International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, 2015.

[69] N. A. Yekini, I. K. Oyeyinka, A. O. Itegboje and A. K. Akinwole, "Automated Biometric Voice-Based Access Control in Automatic Teller Machine," *International Journal of Advanced Computer Science and Applications,* vol. 3, no. 6, pp. 72-77, 2012.

[70] C. Dawson, A Practical Guide to Research Methods, Oxford: How to Content, 2007.

[71] N. William and B. Baiche, Your Research Project: A step-by-step guide for the first-time researcher, SAGE, 2001.

[72] A. Bryman and E. Bell, Business Research Methods, Oxford University Press, 2003.

[73] M. Rouse, "Unified Threat Management," TechTarget, 18 March 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/unified-threat-management-UTM. [Accessed 17 October 2018].

[74] SANS, "Encryption," in *Security 401: SANS Security Essentials Bootcamp Style*, SANS Institute, 2011, pp. 10-13.

[75] Z. Lovric and I. Sedinic, "Influence of Established Information Security Governance and Infrastructure on Future Security Certifications," in *36th International Convention on Information and Communication Technology, Electronics and Microelectronics*, Chicago, 2013.

[76] E. N. Kasanda and J. Phiri, "ATM Threats: A Case Study of Emerging Threats," *International Journal of Advanced Studies in Computer Science and Engineering,* pp. 1-7, 2018.

APPENDICES

A1: Introductory Letter

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

10 April, 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

RE: ELLA NSONTA KASANDA- 2016145967

This is to confirm that the bearer of this letter **Ms Ella Nsonta** Kasanda is a Master of Engineering Student in ICT Security at the University of Zambia, in the School of Engineering, Department of Electrical and Electrical Engineering.

She is currently conducting a research titled "**Investigation of the Level of ATM Security in Zambia based on Payment Card Industry Data Security Standards.**"

We will be most grateful for any assistance you may render to her as she carries out this academic assignment.

The School commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Balimu Mwiya
ACTING ASSISTANT DEAN (POST GRADUATE) - SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

Excellence in Teaching, Research and Community Service

A2: Questionnaire

The University of Zambia

School of Engineering

An Investigation of the Level of Security on Automated Teller Machines in Zambia based on Payment Card Industry Data Security Standard (PCI DSS)

By Ella Nsonta Kasanda (2016145967)

Master of Engineering – ICT Security

For further details or any queries, kindly get in touch on 0972 702 715

Dear Respondent,

I am a student at the University of Zambia in my final year pursuing a Master of Engineering – ICT Security. As partial fulfillment for the award of a Master's degree, I am conducting a baseline study on: "**The Level of Security on Automated Teller Machines in Zambia based on the Payment Card Industry Data Security Standard (PCI DSS) and how Security can be enhanced".**

You have been purposively sampled to provide information for the topic indicated above. The information being collected is purely for academic purposes as such, it will be treated with maximum confidentiality. Subsequently, you are not supposed to indicate your name or any personal information that can lead to revealing of your identity.

Your co-operation will be greatly appreciated.

For more information queries in relation to the survey, you may wish to contact the following:

Research Supervisor: Dr. Jackson Phiri on 0966 693 731 or

Assistant Dean: Dr. Mwanaumo on 0969 561 353

Part A: Bio Data - Please tick in the box as appropriate

1) **Sex:** **(a**) Male ☐ (b) Female ☐

2) **Age in years.**

(a) 18 – 22 ☐ (d) 30 – 34 ☐

(b) 22 – 26 ☐ (e) 34 – 40 ☐

(c) 26 – 30 ☐ (f) 40 and above ☐

3) **Marital status**

(a) Single ☐ (d) Separated ☐

(b) Married ☐ (e) Divorced ☐

(c) Widowed ☐

4) **Level of education**

(a) Secondary ☐ (c) University ☐

(b) College ☐ (d) others ☐

5) **Line of specialty,** please specify……...

6) **Professional certifications,** please list them:

……..... ……..

7) **What is your organization's Primary industry?**

(a) Government Agency/Authority ☐ (b) Health Care ☐

(c) Telecommunications/ICT/ISP ☐ (d) Banking ☐

(e) Energy/Utility ☐ (f) Security ☐

8) What is your organization's size in terms of its overall workforce, including employees and outside individuals such as contractors, consultants and interns?

(a) Fewer than 500 ☐ (b) 500 - 999 ☐

(c) 1000 – 4999 ☐ (d) 5000 & above ☐

9) **What is your primary role in the organization?**

a. Security manager/ Director/CSO/CISO ☐
b. ICT manager/ Director/CIO ☐
c. Risk Manager/ Director ☐
d. Compliance officer/ Auditor ☐
e. ICT Specialist ☐
f. Digital forensics ☐
g. Legal professional ☐
h. Security Analyst ☐
i. Help desk agent / technician ☐

j. System administrator
k. Investigator ☐
l. If others, please specify……..

PART A (Tick the correct answer)

1. **Do you think banking would have been better if the ATM was never invented?**

a) Yes ☐

b) No ☐

c) Makes no different ☐

2. **How often do you use the ATM?**

a) On a daily basis ☐

b) Once a week ☐

c) Once a month ☐

3. **How long have you been using the ATM**?

a) Less than a year ☐

b) Greater than one year but less than 3 years ☐

c) More than 3 years ☐

4. **Have you ever heard of ATM fraud?**

a) Yes ☐

b) No ☐

5. **Have you ever been a victim of ATM fraud either as an Individual or as a Bank?**

a) Yes I have been a victim ☐

b) I have not been a Victim , but the Bank has been a Victim ☐

c) No ☐

If Answer to Question 5 is YES, give details

……

……

6. **What does your ATM card have?**

a. CHIP and PIN only ☐

b. Magnetic Stripe only ☐

c. CHIP and PIN with Magnetic Stripe on the back of the Card ☐

7. **If the answer in Question 5 is (a) and answer in Question 6 is (a) or (c), When did you experience the ATM fraud occur?**

a. Whilst using Magnetic Stripe ATM card ☐

b. After being issued with the CHIP and PIN ATM card ☐

8. **Has there been a time when you have forgotten the PIN for your ATM card?**

a) Yes ☐

b) No ☐

9. **How many ATM cards do you own?**

a) 1 ☐

b) 2 ☐

c) More than 2 ☐

10. **If your answer to Question 9 is (b) or (c), Do you use the same PIN for 2 or more of your ATM cards?**

a) No, each ATM card has its own PIN ☐

b) Yes the PIN for 2 ATM cards is the same ☐

c) Yes more than 2 ATM cards have the same PIN ☐

11. Do you share your ATM card or PIN with your spouse?

a) Yes my spouse has access to both my ATM card and my PIN ☐

b) Yes my spouse has access to my ATM card but doesn't know the PIN ☐

c) Yes my spouse knows my PIN but has no access to the ATM card ☐

d) No my spouse has no access to my ATM card and doesn't know my pin ☐

12. How do you store your ATM card PIN?

a) write it down on a piece of paper ☐

b) Save it in my phone ☐

c) I have just memorized the PIN ☐

13. Do you feel ATM terminals in Zambia are safe to use?

a. Yes ☐

b. Yes but an additional layer of security must be added ☐

c. No they are not secure ☐

SECTION B: CHIP AND PIN CARD – (Tick the correct answer)

14. Does your ATM card request for a pin when you use a point of sale (POS) machine?

a) Yes all the time ☐

b) Yes but not all the time ☐

c) No it never requests ☐

15. Have you ever travelled out of the country and used your ATM card on a point of sale (POS) machine?

a) Yes ☐

b) No ☐

16. If answer in 15 is yes, what did you require to complete your transaction pin or signature

a) Always PIN ☐

b) Always Signature ☐

c) Sometimes PIN other times Signature ☐

17. Does your Banks CHIP and PIN ATM cards have data on the magnetic stripe?

a) Yes there is information on the magnetic stripe ☐

b) No there is no information on the magnetic stripe ☐

18. Have you signed up for SMS alerts when money is withdrawn from your account?

a) Yes ☐

b) No ☐

19. If yes do you receive an SMS each time money is withdrawn from your account?

a) Yes always ☐

b) Sometimes ☐

c) Never ☐

SECTION C ATM SOFTWARE (Tick the correct answer)

20. What version of windows are your ATM terminals running on?

a) All are on Windows 7 ☐

b) All are on Windows XP ☐

c) Some are on Windows 7 and others on Windows XP ☐

d) Not sure ☐

21. Do you have a firewall to protect your customers' data?

a. Yes ☐

b. No ☐

c. Not sure ☐

22. What passwords does one require to log onto your ATM?

a. Vendor supplied passwords ☐

b. Password created according to banks password policy ☐

c. Not sure ☐

23. Do you have cardholder data retention policies in place?

a. Yes policies are in place and are being used ☐

b. Policies have been formulated but not yet approved ☐

c. No policies are in place ☐

d. Not sure ☐

24. How do you ensure card holder data is encrypted while being transmitted across open or public networks? (select all that apply)

a. By use of cryptography ☐

b. by ensuring only trusted keys and certificates are accepted ☐

c. by ensuring security policies and operational procedure are documented, in use and known to all affected parties ☐

d. Card holder data is not encrypted ☐

e. Not sure ☐

25. Who loads encryption keys on your ATMs?

a) Only bank employees ☐

b) ATM Vendors ☐

c) Bank employees or ATM Vendors ☐

26. Do you have an anti-virus installed on all the ATM terminals on the network?

a. Yes it is installed on all the ATM ☐

b. Yes it is installed but not on all ATM terminals ☐

c. No its not installed ☐

27. How often do you update the anti-virus?

a. On a daily basis ☐

b. Once a week ☐

c. Once a month ☐

d. Once every 3 months ☐

e. Never ☐

28. How often do you perform period scans on the ATMs?

a. Once a month ☐

b. Once every 3 months ☐

c. Once every 6 months ☐

d. Never ☐

29. Do you generate audit logs for ATMs and retain them?

a. Yes ☐

b. Generate audit logs but don't retain them ☐

c. No ☐

30. Does any ATM vendor have access rights to disable or uninstall the anti-virus on the ATM terminal?

a. Yes the vendor installs software on the ATM terminals ☐

b. No the ATM vendors only have access to the ATM hardware ☐

c. ATM vendor has access to the ATM software but work under bank employee supervision ☐

d. Not Sure ☐

31. Do you have any policies and operational procedures for protecting ATMs documented?

a. Yes ☐

b. Yes but not yet approved ☐

c. No ☐

d. Not Sure ☐

How often do you do vulnerability and Risk assessments on your ATMs?

a. once a quarter ☐

b. twice a year ☐

c. Once a year ☐

d. Never ☐

e. Not sure ☐

32. Do you know what ATM card Shimming is?

a) Yes I know ☐

b) I have heard of it but I don't know what it is ☐

c) No I have never heard of it ☐

33. Have you ever heard of ATM Jackpotting?

a) Yes I know ☐

b) I have heard of it but I don't know what it is. ☐

c) No I have never heard of it. ☐

34. Do you feel Zambia is cyber ready for Shimming and Jackpotting attacks?

a) Yes it is. ☐

b) No its not ready ☐

c) Not Sure ☐

Thank you very much for contributing to my Research
God bless you