

**DIGITAL LENDING AND INFORMATION SYSTEM SECURITY IN  
KENYA**


**CATHERINE MONG'INA ONSANDO**

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF  
BUSINESS ADMINISTRATION (MBA), FACULTY OF BUSINESS AND  
MANAGEMENT SCIENCES, UNIVERSITY OF NAIROBI.**

**2021**

## DECLARATION

This project is my original work and has not been presented for a degree in any other university.

Signature.....  .....

Date...25<sup>TH</sup> NOVEMBER 2021.....

**Catherine Mong'ina Onsando**

**D61/10426/2018**

This research project has been submitted for examination with my approval as the University supervisor.

Signature . 

Date: 3<sup>rd</sup> December 2021

**Dr. James T. Kariuki**

**Senior Lecturer, Department of Management Science**

## **ACKNOWLEDGEMENT**

Praises and thanks to God for His able provision and strength throughout this period. I would like to express my deepest gratitude to my supervisor Dr. J.T Kariuki for his guidance throughout this research.

Special thanks to my late Aunt Ms. Rose Onsando for always believing and supporting my dreams. Her encouragement, continuous moral and psychological support were unmatched.

Throughout this research there are many others who have been very supportive and I would like to extend my appreciation to them too.

## **DEDICATION**

To my late aunt Ms. Rose Margaret Sarange Onsando.

## TABLE OF CONTENTS

<b>DECLARATION.....</b>	<b>ii</b>
ACKNOWLEDGEMENT .....	iii
DEDICATION.....	iv
TABLE OF CONTENTS.....	v
LIST OF TABLES .....	viii
ABBREVIATIONS AND ACRONYMS.....	ix
ABSTRACT.....	x
<b>CHAPTER ONE: INTRODUCTION.....</b>	<b>1</b>
1.1 Background of the Study .....	1
1.1.1 Information Security.....	3
1.1.2 Information Security Threats .....	4
1.1.3 Adoption of Information Security Control Measures .....	4
1.1.4 Challenges of Securing Information Systems .....	5
1.1.5 Digital Lending in Kenya.....	6
1.2 Research Problem .....	8
1.3 Objectives of the Study .....	10
1.4 Value of the Study .....	11
<b>CHAPTER TWO: LITERATURE REVIEW.....</b>	<b>12</b>
2.1 Introduction.....	12
2.2 Theoretical Foundation .....	12
2.2.1 Technology Acceptance Model (TAM).....	12
2.2.2 The General Deterrence Theory.....	13
2.2.3 Integrated System Theory.....	14
2.2.4 The Information Security Management Theory .....	15
2.3 Information Security Threats .....	15
2.4 Information Security Systems Adopted by Digital Lenders.....	16
2.4.1 Encryption .....	16
2.4.2 Permission Based Access.....	17
2.4.3 Two factor Authentication .....	18
2.5 Challenges in Securing Information Systems .....	19
2.5.1 Lack of Financial Resources.....	19

2.5.2 Inadequate ICT Staff Skills .....	20
2.5.3 Complexity of Information Systems .....	22
2.5.4 Lack of Top Management Support .....	23
2.6 Summary .....	24
<b>CHAPTER THREE: RESEARCH METHODOLOGY.....</b>	<b>26</b>
3.1 Introduction .....	26
3.2 Research Design .....	26
3.3 Population .....	26
3.4 Data Collection.....	26
3.5 Data Analysis .....	27
<b>CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION.....</b>	<b>28</b>
4.1 Introduction .....	28
4.2 Response Rate .....	28
4.3 Demographic Characteristic of Respondents .....	28
4.3.1 Distribution of Respondents by Age and Highest Education Level .....	28
4.3.2 Distribution of Respondents by Position Held and Work Experience.....	29
4.4 Organizational Information .....	30
4.4.1 Distribution of Respondent’s Firm by Duration of Operation .....	30
4.4.2 Distribution of Respondent’s Firm by Sector and Ownership Structures .....	31
4.4.3 Distribution of Respondents by Size of Respondents Firms .....	31
4.5 Information Security Threats Faced by Digital Lenders in Kenya .....	32
4.6 Information Security Measures Adopted by Digital Lenders in Kenya .....	39
4.7 Challenges Faced by Digital Lenders in Securing their Information Systems .....	44
4.8 Discussion of Findings .....	52
<b>CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.....</b>	<b>55</b>
5.1 Introduction .....	55
5.2 Summary .....	55
5.3 Conclusion .....	56
5.4 Recommendations.....	56
5.5 Recommendations for Further Study.....	57
5.6 Limitations of the Study .....	57

<b>REFERENCES</b> .....	<b>58</b>
<b>APPENDICES</b> .....	<b>65</b>
Appendix I: Digital Lenders in Kenya .....	65
Appendix II: Questionnaires .....	67

## LIST OF TABLES

Table 4.1: Distribution of Respondents by Age .....	29
Table 4.2: Distribution of Respondents by Highest Education Level .....	29
Table 4.3: Distribution of Respondents by Position Held in their Organization .....	30
Table 4.5: Distribution of Respondent's Firm by Ownership Structures .....	31
Table 4.6: Distribution of Respondents by Size of Respondents Firms .....	32
Table 4.7 Rating of Information Security Threats.....	32
Table 4.8: Total Variance Rating of Information Security Threats .....	34
Table 4.9: Rotated Component Matrix of Information Security Threats .....	35
Table 4.10 Rating of Information Security Measures Adopted.....	39
Table 4.11 Total Variance Rating of Information Security Measures Adopted .....	40
Table 4.12: Rotated Component Matrix of Information Security Measures Adopted .....	41
Table 4.13: Rating of Information Security Challenges .....	45
Table 4.14: Total Variance Rating of Information Security Challenges .....	46
Table 4.15: Rotated Component Matrix of Information Security Challenges .....	47



## **ABBREVIATIONS AND ACRONYMS**

<b>CIA</b>	:	Confidentiality, Integrity and Availability
<b>DDoS</b>	:	Distributed Denial of Service
<b>EMP</b>	:	Electromagnetic Pulse
<b>HTTPS:</b>		Hypertext Transfer Protocol Secure
<b>ICT</b>	:	Information and Communication Technology
<b>IFMIS:</b>		Integrated Financial Management Information System
<b>IS</b>	:	Information System
<b>ISS</b>	:	Information System Security
<b>IT</b>	:	Information Technology
<b>KCB</b>	:	Kenya Commercial Bank
<b>MIS</b>	:	Management Information Systems
<b>MVNO:</b>		Mobile Virtual Network Operator
<b>PU</b>	:	Perceived Usefulness
<b>PEOU:</b>		Perceived Ease of Use
<b>SSL</b>	:	Secure Sockets Layer
<b>TAM</b>	:	Technology Acceptance Model
<b>TLS</b>	:	Transport Layer Security
<b>USSD</b>	:	Unstructured Supplementary Service Data

## ABSTRACT

Today, information is regarded as a valuable resource for any organization and with the advent of globalization and ever-changing technologies, the need for information security is becoming more and more critical. The importance of information system security is getting more noteworthy as firms are becoming reliant on information technology. While originally information security was regarded as a technology hiccup that could be addressed through refined hardware together with software answers, rise in the number of security gaps demonstrates that this is also a people problem. The overall objective of this study was to establish adoption of information system security among digital lenders in Kenya. The specific objectives were to determine information security threats faced by digital lenders, information security measures adopted by digital lenders and establish challenges faced by digital lenders in securing their information systems. The population of the study was the 29 registered digital lenders in April 2021. Primary data was collected through the use of closed ended questionnaires. Out of the 29 questionnaires administered, 16 were received back resulting in a 55.17% response rate. Data was analysed through the use of mean, standard deviation and factor analysis. The study findings revealed that the major information security threat faced by digital lenders was phishing. To counter threats in the sector, the three major information security measures adopted by digital lenders were automatic logout policy for workstations after a predetermined period of inactivity; password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols; and application of firewalls that enforce a secure boundary between the internal network and the Internet. The study findings also revealed that there were two major challenges faced by digital lenders in securing their information systems namely lack of awareness by customers on the risk of sharing their passwords and lack of information security awareness amongst customers. Recommendations to digital lenders are to enhance customers' awareness on the risk of sharing their passwords and to be more security conscious as they use digital lending systems. In addition, digital lenders should enforce security measures as such automatic logout, password complexity requirements policy and application of firewalls.

# CHAPTER ONE

## INTRODUCTION

### 1.1 Background of the Study

Today, information is regarded as a valuable resource of any organization and with the advent of globalization and ever-changing technologies, the need for information security is becoming more and more critical. The importance of Information System Security (ISS) is getting more noteworthy as firms become reliant on information technology. While originally information security was regarded as a minor setback that could be addressed through refined hardware together with software answers, rise in the number of security gaps reveal that it is also people problem (Rudolph, 2002). In this regard managing information risks requires shared responsibility of persons within the organization which include, oversight administration, and everyday operations providing adequate reaction measures to sufficiently protect the missions and business functions of these companies (NIST, 2011).

Effective risk management requires that organizations achieve an ideal equilibrium on maximizing their opportunities for gain while minimizing susceptibilities and loss. This is accomplished mostly by warranting that the influence of risks exploiting susceptibilities is within satisfactory limits at an affordable cost to the organization (NIST, 2011). It can be debated that because security of information is continually evolving, businesses have embraced information security as a vital countermeasure. Further, they have become increasingly dependent on vulnerable networks such as the cloud to convey delicate data and information. Guarding data and information is consequently less focused on the technology and more on sustainability of the business itself.

Various theories have been fronted to explain the information security phenomenon. The Technology Acceptance Model (TAM) according to Davis (1989), shapes how users of information technology come to reach an agreement and use a technology, therefore suited to adoption of information security. The General Deterrence Theory symbolizes a human shared intention and ought to consider morals, deeds together with partialities (Nagin, 1978). Customers, shareholders together with other people can have a solid impact on a business and ought to be well thought-out within the security parameters. The Integrated Systems Theory emphasizes on the organization strategy and design (Hong et al., 2006). It explores the interactions between people, assets and processes working towards a shared objective. Processes, ethos together with architecture of an organization are vital in shaping the design of the information security strategy. Lastly, the Information Security Management Theory echoes upon the processes that recognize ration together with control risk, obtainability, integrity, and discretion, and they in addition warrant answerability (Finne, 1998).

Digital lending denotes the use of digital means to process and advance loans directly to individuals and small business (Francis, Blumenstock, & Robinson, 2017). It leverages digital infrastructure and involves limited in-person contact. In Kenya, 77% of borrowers have taken only digital loans which reflects the wider accessibility and reach of digital lending for borrowers (FSDK, 2018). Design and delivery mechanisms of digital lending are through mobile banking, mobile money, unstructured supplementary service data (USSD) and mobile applications. Concerns around access to, use, storage, and sharing of alternative data obtained from consumers are on the rise. Nyawira (2020) noted that digital lenders are found to be exploiting borrowers “insider information” and act which is a breach of privacy. Consequently, in the attempt to recover outstanding debts, some money lenders get information from their client’s contact list encouraging their links to push the loaned to pay their liability without their

client's permission. It is therefore important to examine the role of information security in this growing environment and to recognize possible threats together with areas of development, with the general objective of shielding system operators together with reinforcing the security obstacles that will permit this new range of digital fiscal providers to become dependable, safe and consistent.

### **1.1.1 Information Security**

Security of information systems entails guarding information and assets from unapproved access, use, interference, alteration or damage (Larsen, Pedersen & Andersen, 2006). The Confidentiality, Integrity and Availability (CIA) model provides guidance on rules for security of information in an organization. The principles of the CIA triad form three important modules of information security (Gibbard, 2005). Information confidentiality entails data and information being shared only amongst authorized individuals. Confidentiality breaches can happen when information is disclosed either by word of mouth, during transmission of information via e-mail, copying, or creating documents and other data. Information integrity refers to authenticity and completeness of information. It ensures that the data being accessed or read, has neither been tampered with, nor been altered or damaged by an individual or through a system error over its entire life-cycle.

Information integrity is a key component of security information. Thus, information security is needed so to have a comprehensive security management system. Lastly, availability means that the information security systems responsible for information collection, processing and storage are easily accessible when required, by those who require them (Schmandt et al. 2019).

### **1.1.2 Information Security Threats**

In Information System Security, system weaknesses can be exploited by threats to breach security and negatively modify, delete or cause harm to data and information. They can be categorized as either internal or external threats. Researches have shown that the human aspect of information security has not in the past been given ample attention and yet many of the breaches are as a result of people and processes. Enterprises are faced with threats perpetrated by insiders with clear malicious intent (Brandin et al., 2004).

External threats that are aided by insiders pose as a significant information security risk challenge due to the existing weaknesses in the security framework. External threats such as malware, adware, phishing, DDoS attacks, ransomware; are just some of the methods used to externally gain unauthorized access to data and information. According to Pereira (2016) a serious impact on business profitability, reputation, customer satisfaction, confidence, and economic growth can be a consequence of theft and loss of organizational information. Physical security threats that may cause harm to systems include terrorism attacks, deluges, fires earthquakes and tremors. To counteract these threats, organizations should utilize defensive mechanisms to endorse integrity, availability, and confidentiality, without disrupting the functionality together with the usability of Information Systems (IS).

### **1.1.3 Adoption of Information Security Control Measures**

To ensure confidentiality, integrity and availability of systems, secure and efficient operation of information together with adequate execution of the security controls is vital to the firm. Controls are essentially a set of guidelines, processes, strategies, practices or governmental arrangements used for safeguarding information systems (Rainey, 2015). They are one of the primary methods of managing information security risk and a major responsibility of

information security management. Typically, organizations identify and select security controls as per their organization's wants together with the associated security needs. A cost-benefit investigation ought to be carried out to determine that the implementation expenses of the controls can be vindicated by the lessening in the degree of risk (Rainey, 2015).

To achieve reasonable assurance in information security appropriate counter measures such as file authorizations together with user admission controls can be applied. Version control additionally can be implemented to mitigate against flawed changes or even accidental deletion by users that are permitted to use the system. Other counter measures that can be implemented in case of system errors like an electromagnetic pulse (EMP) or server malfunctions like checksums, certificates, logging and digital signatures to verify reliability. Backups and redundancies ought to be in place to reinstate information to its right state. Information security is therefore aimed at protecting information from threats through use of appropriate controls (Oinas-Kukkonen & Harjumaa, 2009).

#### **1.1.4 Challenges of Securing Information Systems**

Information as an asset can bring forth challenges such as costly hardware acquisitions to process and store the data. In addition, insufficient financial resources to develop, implement and maintain information security is often a significant challenge for organizations. In his study, Muhati (2018) highlights nonexistence of monetary assets, none existence of top management support, and lack of skills or required competence and information system characteristics as challenges that inhibit adoption of information security within an organization. Adopting and implementing information security measures in an organization requires adequate financial resources. Many organizations do have adequate budget when it comes to IT operations. The budget for information security should be adequate to allow for

scalability to meet future demand (McLaughlin & Gogan, 2018). To curb the challenge, the firm must align their information security budget with the strategy of the business.

Further, like any other enterprise, security of information touches on of governance together with continuing support for it to prosper. Any indifference, disregard or utter aggression is probable for it to end in unpleasing results. Top management must be involved in every step of adopting the information security strategy starting from planning to maintenance. Finally, a research by Barki et al., (2015) opined that non- existence of user commitment, unproductive communications with information system users, clashes amongst user divisions together with absence of information security skills amongst employees are all a slowdown to application of MIS systems in organizations. There is need therefore for each organization to position itself at a good ICT literacy level.

#### **1.1.5 Digital Lending in Kenya**

Digital lending, since its launch in 2012, serves over 35% (approximately 7 million people) of the number of adults who own a mobile phone in Kenya (Kashangaki, 2020). Digital lending main features include immediate loan access, computerized credit choices together with a remote payment and compensation, making it a fast, private, plus opportune choice for a good number of debtors. There were 29 digital lenders in Kenya in April 2021 spread across various industries including Banking, Fintech and Microfinance. The Digital Lenders Association of Kenya (DLAK) was incorporated in 2019 to consolidate digital loan providers together with associated shareholders to enable mutual development in the digital lending industry.



Digital lending in Kenya is rendered via three business models. According to Hwang and Tellez (2016) the initial business model and the most popular is the partnering of banks or microfinance firms and mobile network users. Such kinds of businesses include Safaricom M-Pesa together with Commercial Bank of Africa to offer MShwari, Safaricom M-Pesa together with Kenya Commercial Bank to offer KCB-M-Pesa loans and Co-operative Bank of Kenya to offer MCoop Cash advances. Application based digital lending is the other type of business model. It entails organizations providing loans in their own name without partnership with financial organizations. Leading app-based lenders (such as Tala, Branch and Saida) account for less than 10% of the market.

The third model is where a bank offers digital services. This model is not very common though. This business model started because of Central Bank of Kenya licensing Mobile Virtual Network Operators (MVNO). With this model banks need not partner with mobile network operators as they can come up with a digital infrastructure that is their own. Equity Bank is an example in this category. Equity bank, the leading lending institution by depositors, disburses USD 0.57 billion via their Equitel Eazzy Loan platform every year (FSDK, 2018). Their telecommunication infrastructure is a lease from Airtel Kenya. A good number of digital borrowers have loans given by M-Shwari which controls the Kenyan digital lending market share at 29%. Tala and Branch, the two leading app-based digital loan products businesses have equally taken around 6.7% of the digital market share that comprises 1.3 million individuals on the estimate.

Digital loans have changed the marketplace for credit in Kenya in the recent past. Mobile phones, identity-linked digital footprints, computerized credit scoring; agent systems together with credit data sharing – digital lending the building blocks have facilitated providers offer

loans swiftly and at scale. However, concerns have been on the rise in regards to access to, use, storage and sharing of alternative data obtained from consumers. Security of information is therefore of paramount importance especially to the digital lending sector and this forms the motivation behind the study to evaluate digital lending and information system security in Kenya.

## **1.2 Research Problem**

Organizations utilize data protection because they must protect their communication applications and networks in cyberspace in order to continue providing high-quality services and goods to their consumers (Kumar, 2011). The study area of information security is about privacy, integrity together with availability of information assets. Information Systems (IS) constantly face internal and external threats and digital lending platforms are not spared from this onslaught. Breaches to digital monetary lending platforms may endanger customer's personal data such as credit history, email addresses, phone numbers and location history. There exist numerous unresolved problems regarding effectual security of information systems amongst digital lenders in Kenya such as insufficient financial resources to develop, implement and maintain information security tools, none existence of top management support, lack of skills or required competence and information system characteristics.

As Sipior and Ward (2008) notes, the use of the World Wide Web has brought with it growth of uncertainties which include buyer self-assurance in online trade doings, dangers to information integrity, lawful liability together with the possibility of suffering monetary loss. With the dramatic increases of hacking of websites in Kenya and state of data and information compromised, more effective information security tools and services need to be introduced and implemented (Cyber Security Overview, 2019). As a result, a company's consideration of these

concerns is vital while establishing information security in the enterprise. It also allows for new and improved ways to execute electronic transactions, lowering operating costs by ensuring predictable results and decreasing risk factors that may disrupt the process. Other advantages include security against customer and revenue loss as a result of reduced staff production and inability to satisfy corporate needs. Considering the aforementioned context, concerns around major information system security threats, challenges of adopting information systems security and existing information systems security adopted by digital lenders forms the motivation behind the study to examine digital lending and information system security in Kenya.

Ng and Kwok (2017) examined the arrival of Fintech together with cyber security in a global monetary center. The study revealed that though they may not be held to the same regulations as traditional banks, they must follow privacy laws. Pereira and Santos (2014) examined the challenges in information security protection. The study revealed that nurturing together with unceasingly encouraging a security values plus acknowledging that individuals still are, and will forever be the feeblest link, will surely help firms to attain their satisfactory levels of security. This will consequently lead the business being closer to attaining their business objectives.

Muratha (2012) did a study on security of information doings in the Kenyan capital marketplace. The findings of the study revealed that security is generally more than just a technological problem. Previous studies have shown that the human facet of security of information has not been provided much attention and yet many of the breaches being faced are on people and processes. Further, he points out that with the dramatic increases of hacking of websites in Kenya, the state of data and information being compromised, more effective information security tools and services need to be introduced and implemented.

Njiru (2013) conducted research in Kenya on information security activities in the banking business. Human stakeholders were found to be the greatest danger to information system security, according to the study (Njiru, 2013). Kitheka (2013) conducted research on information security management systems at Kenyan public universities. The study found that public university information security procedures were insufficient to cope effectively with information security risks (Kitheka, 2013). Ngalyuka (2013) performed research into the relationship between ICT usage and fraud damages in Kenyan commercial banks. According to the findings, the use of ICT has exposed Kenyan commercial banks to more fraud (Ngalyuka, 2013).

Although researches had been done on data security, most argued within the context of service delivery in banks, none focused on digital lending and information system security in Kenya. The study questions, therefore, are: What are the major information security threats faced by digital lenders in Kenya? What are the existing information security measures adopted by digital lenders in Kenya? What are the challenges encountered by digital lenders in securing their information systems?

### **1.3 Objectives of the Study**

The overall aim of this research was to establish adoption of information system security among digital lenders in Kenya. Specifically, the study sought:

- i. To determine information security threats faced by digital lenders.
- ii. To determine information security measures adopted by digital lenders.
- iii. To establish challenges faced by digital lenders in securing their information systems.

#### **1.4 Value of the Study**

The results of this research are of great importance to digital lenders in Kenya. It will give insights into information security threats, importance of information security and challenges faced in securing information systems. It will enable them to formulate appropriate strategies, guidelines and standards to safeguard information.

Policy makers such as Central Bank of Kenya will use the findings to form a background for development of guidelines and standards for digital lending firms in Kenya which can be implemented for better service delivery.

The research will be significant to academicians and researchers since this research will contribute to the body of knowledge on information security threats, information security controls together with cyber safety in addition to providing reference material to scholars. The research findings will form a basis for further studies on challenges of information security adoption.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1 Introduction**

This section explains the relevant literature on information security; specifically, the literature review focuses on theoretical foundation of information system security as well as various factors affecting information system security.

#### **2.2 Theoretical Foundation**

Various concepts have been fronted to elucidate the information security phenomenon. Four theories provided the basis for the research: Technology Acceptance Model (TAM), general deterrence theory, integrated system theory and lastly, the Information security management theory. The TAM model supported the study by elucidating how users come to accept and use a technology. The general deterrence theory emphasizes on impact customers, shareholders together with employees have on information security. The integrated system theory fronts for softer approaches in implementing information security. Lastly, the information security management theory supports the study by articulating how organizations that uphold information security do so by executing advanced controls. The theories are deliberated below.

##### **2.2.1 Technology Acceptance Model (TAM)**

According to Davis (1989), the Technical Acceptance Model (TAM) has been used to explain the dissemination of innovations ranging from new farming practices to current communication technologies. The Technology Acceptance Model's basic concept is that the more accepting consumers are of innovative structures, the more willing they are to make time and effort adjustments to essentially begin utilizing the system.

Davis (1989) argued that a client's willingness to accept a new technology was determined by their perceptions of simplicity of use and utility. Apparent effectiveness might refer to the degree to which it is thought to aid or enhance a person's capacity to do their duties more effectively. The apparent ease of use refers to the amount of effort required to utilize an application. If a person feels a system is easy to use, he or she is more likely to install and use it. This theory's belief constructions – Perceived Ease of Use (PEOU) plus Perceived Usefulness (PU) – thoroughly disclose the impact of external variables including innovation and personal attributes on IT usage behavior.

TAM can be used to endorse worker implementation and use, together with compliance with information security measures in order to inspire positive attitude in the direction of those measures. In the context of information security, as organisations are dedicated on shielding their firms from the susceptibilities of external risks, they can also focus on employee's ease of use of information security processes.

### **2.2.2 The General Deterrence Theory**

The General Deterrence Theory fronts that individuals select to follow or not to follow the regulation after computing the advantages together with penalties of their deeds (Cohen, 1978). The theory, posits consumer responsiveness of information safety countermeasures, and severity of restrictions associated with information system misuse. According to this theory, the more likely it is to get punished the stronger the sanctions are, the better employees behave (Rao & Herath, 2009). A key assumption of this theory is that offenders weigh up the pros and cons of a certain action and make their own rational decisions.

As such, this concept of deterrence theory can leverage deterrence techniques such as policies and guidelines given to employees to change their passwords in a certain time frame. According to Nance and Starub (1988) an important application of the deterrence concept is established on the association amongst managers together with computer abuser and their activities. Thus relevance to the study is premised on information security controls being used as a tool by management to implement deterrence methods. Gibbs (1975) states that the stronger the severity and certainty of sanctions of certain behavior; the more individuals are deterred by it. The outcomes submit that practices that discourage information abuse are consumer consciousness of security, guidelines, security training, and computer expertise. In the country, it reflects upon the basic fundamental human intentions expected towards embracing measures that will ensure data safety and prosperity. The theory captures the ethical exuberance concerning the existing information security governance structures.

### **2.2.3 Integrated System Theory**

The theory as per Hong et al. (2003) on the other hand postulates the merits of combined system theory in undertaking information safety management approach and management outcome fixes. The theory explores the very many unprecedented security challenges faced by organizations and decries a lack of security management frameworks. It proposes combination of risk, contingencies, assessing together managing policies concepts to build an all-inclusive theory of Information Security Management. The theory advocates for a more unified and management approach in handling information security issues holistically. Relevance to the study is premised on the very many unprecedented security challenges organizations are facing, and the relevant approaches adopted to ensure information is managed in the most effective ways. The domain of information security systems presents a strategic problem that remains a



challenge for most senior managers (Clarke, 2012). The Integrated System Theory fronts for softer approaches in implementing information security systems.

#### **2.2.4 The Information Security Management Theory**

Information Security Management Theory discloses the wider complexities of an interdisciplinary nature; highlighting the importance of having an adequate understanding of the various concepts of information security risk management (Finne, 1998). The model identifies critical business organizational processes and internal controls of information security risk management. Eloff & Eloff (2003) stated that the optimal way to combine products and processes for information security is by defining a code of practice during the evaluation process. Solms (2004) identifies key aspects to avoid mistakes and serious errors in the evaluation process of information security management from different viewpoints. The scholars view information security as an organizational responsibility and regard data protection as a business issue rather than a technical problem. The model, articulates how business processes are a foundation of prosperity in those organizations that uphold information security by injecting the aspect of enhanced processes and controls.

#### **2.3 Information Security Threats**

Threats have the ability to act against an asset in a way that can lead to danger. They potentially cause an unwanted incident (ISO/IEC 13335-1:2004, 2010). In this setting, threats are any circumstances or happenings with the possibility of causing harm to an information resource by take advantage of susceptibilities in the information system. They may originate from internal or external sources.

A significant number of internal threats are caused by employees' leading to intentional or unintentional harm. IS systems have trusted individuals. If one of those trusted individuals chooses to break the trust it can be problematic to forecast or stop (Shelley, 2015). The usual internal threat is an existing or past employees, supplier or business associate who has certified entry to the organizations information systems, data or networks (Wimmer, 2015). Intentional harm may be caused when a disgruntled employee compromises systems or releases data exposing the firm to legal or reputational damage. A worker who has just been downgraded or sidestepped for a raise could also pose a significant threat.

External threats to IS can originate from anywhere and may take on many forms such as social engineering attacks, DDoS attacks, malware, spyware, adware or viruses. External threat actors include hackers or advanced persistent threats that are skilled and determined to break into systems for economic purposes (SentinelOne, 2019). Majority of external breaches of security are as a consequence of aims of chances rather than resolute risks. The extent of an organizations exposure ought to be out in mind as it affects the likelihood that susceptibility will be exploited. When vulnerabilities exist in an IS there is a potential risk of external threat exploitation (Watts, 2020).

## **2.4 Information Security Systems Adopted by Digital Lenders**

### **2.4.1 Encryption**

Privacy of information transmitted through the internet is attained by cryptography. As per Soofi, Khan and Fazal-e-Amin (2014) data cryptography refers to the inter-changing of the information of the data, like text, image, audio, video to make the information pointless, incomprehensible or unseen during communication or storing process. The process of transforming data into cipher text is called encryption while the process of reversing the cipher

text back to its novel state is referred to as decryption. The process of encrypting the data with a secret key before exchange or transmission provides an additional layer of security between the sender and receiver (Singh & Jauhari, 2012). Soofi, Khan and Fazal-e-Amin (2014) explain that the key part of encryption is protecting the information from online hackers. Digital lending industry in Kenya has adopted encryption mainly by means of HTTPS, clearing cache and TLS/SSL. HTTPS is being used by all digital lending firms sampled for this study.

The protocol is designed for secure communications over computer networks as well as the internet. Further we noted, Tala and Branch mobile applications utilize Transport Layer Security (TLS) X.509 certificates for the public and private key encryption. Clearing app cache especially on Android devices helps to resolve problems that may arise from corrupted cache data.

#### **2.4.2 Permission Based Access**

Hayikader et al. (2016) define permissions based access control to involve granting a stack of consents for every request and then limiting every request to retrieving device information/data systems that are fall inside the range of those consents and blocking the applications if they attempt to perform actions that exceed these permissions. Putting this into the perspective of mobile phone applications, Felt, Greenwood and Wagner (2011) writes that to guard operators from the risks related with third-party codes, contemporary mobile stages use permission request to regulate admission to security together with confidential applicable portions of the systems. The smartphones are programmed such that users can choose if they want to allow individuals applications to access delicate information.

In the case of digital lending apps operating in Kenya such as Branch, once a user signs up to their service and accepts their terms and conditions the app can access a mobile user's contact list, present locality (via GPS data), SMS together with much more. It is known that digital finance suppliers depend on these types of information so as to make their credit verdicts. For instance, in the case of Tala, they explicitly request permission to collect personal data on your calls and text messages before the process your loan applications. Of concern, even the handful of customers who read and understand the requests for permissions do not understand the implications of the data collected.

### **2.4.3 Two factor Authentication**

As the use of digital lending rises, the security together with privacy risks via malwares, hacking, unlawful access plus mobile fraud surges. According to Dmitrienko, Liebchen, Rossow and Sadeghi (2014), in this setting traditional authentication and password verification is regarded as insufficient in securing critical applications. By distributing the single authentication element, two-factor authentication systems guarantee a better level of security.

According to a study on mobile banking security in Oman by Musaev and Yousoof (2015), two factor authentication has shown to be a safe approach for client verification since it forces consumers to provide extra credentials in combination to existing unique login identifier and password. Two-factor authentication refers to two forms of identification, a thing you are aware of like a password and a thing that you possess like a mobile phone device. In this context, digital lenders in Kenya have employed two-factor authentication by requiring users to insert passwords before completing a transaction. For instance, M-Shwari customers are required to use their unique passwords as a way of verifying that they are whom they claim to be. Digital lenders in Kenya have utilized various variations of Two-factor authentication.

## **2.5 Challenges in Securing Information Systems**

### **2.5.1 Lack of Financial Resources**

Information security countermeasures are frequently a high cost proposition that entail business and technical decisions. According to Ravichandarani (2016) in his study which entailed single users of IS in twenty firms in Miami. The research revealed that contributing to unsuccessful MIS executions included factors like cost overruns, missed time limit, imprecise features together with out-and-out failure. From the results, it is imminent that cost factor affects the implementation of MIS in companies. Numerous firms particularly the small ones cannot risk adopting costly or expensive information security systems of which they are not convinced of their advantage.

Bakos and Brynjolfsson (2015) research posited that MIS technology is usually implemented to decrease synchronization expenses, increase efficiency, or in reply to the demands of influential trading associates. In conjoining, an internet for example makes communications amongst sections, persons, or organizations more inexpensive in comparison to one having to go round or writing letters to relay a message. Using computers makes tasks easier plus quicker in contrast to the ancient approaches of writing together with storage of data that are all the time wearisome, clumsy, pricy together with more time consuming.

According to Clemon and Row (2015), numerous dealers establishments that execute IS technology do so solely at the persistence of an overriding client and as a result, the company obtains little or no benefit. Implementation is expensive for the named organizations but this is essential to reserve the prevailing business association, with the leading business associate intimidating to deny business if application does not happen within a stated period.

According to Dacovou et al. (2014), these organizations are referred to as coerced adopters because there are nonexistence ongoing advantages that are related with the present new information system besides continual business. The said adopters have a robust inducement to make a low-expense, one-off asset in information system technology. These organizations in short will choose a low expense resolution, and once bought, decrease the continuing expenses by not preserving the system technology. The low price of this solution proposes that administration participation will be negligible besides endorsing the package chosen, and that this technology will not be adapted with other information systems.

### **2.5.2 Inadequate ICT Staff Skills**

Information literacy has been defined by Bruce (2002) as “the skill to access, assess, bring together and use data to study, problem solve, make conclusions in formal and casual learning circumstances, at work, at home together with when in educational situations”. Plotnick (1999) defines literacy of information as “the skill to identify when data/ info is required and the ability to trace, assess together with efficiently implement it”. Doyle (1992) on the other hand explained data literacy as “the capacity to access, evaluate and use information/data from a number of sources”. There is need therefore for each organization to position itself at a good information literacy level for it to identify what information is relevant or irrelevant to their business dealings.

The research by Barki et al., (2015) about MIS implementation, showed that that absence of proficiency, expertise, application specific knowledge together with nonexistence of user knowledge on information system adds to MIS development threat. Ewusi-Mensah (2015) explains that for executives to work competently in executing the data system management in their firms, they ought to have a hand and knowledge in information management systems.

Other researches like Block (2015) and Keil et. al (2007) carried out research on interferences to operative implementation of MIS in companies in the United States of America.

The research revealed that absence of user commitment and ineffectual communications with customers are all interference to operative implementation of MIS system in firms.

University of Nairobi carried out a research on the factors influencing operational application of integrated financial management information security systems (IFMIS) in Kenyan governments found out that operative use of the information of data systems are mainly influenced by disruption together with confrontation. The research in addition found out that management support is nonexistence and topmost administration does not motivate the operator. The capacity together with the technical knowledge was established to be little because of nonexistence of teaching together with rushed implementation of the information systems. This research came up with recommends like government to employ a change agent to supervise the operation of the IFMIS structure. In addition, those people who use the information system to undertake a job training to develop their abilities together with capabilities to use the information system (UoN, 2013).

Borura (2010) research was on MIS implementation in Kenyan parastatals. This research used a research design identified as a survey research design. This study design was favored since the investigator planned to gather cross sectional information on the practice together with hindrances of security of information systems application in government parastatals owned companies in Kenya. Even though survey research design was time consuming, the research design was valuable since it permitted contrasts to be made with ease from the findings. The study established there being concerns associated to nonexistence of sufficient teaching

between the employees who interact with the MIS system. The research suggested that trainings be carried out near the time of actual installation. As per the research, it is not resourceful to educate individuals on a new system more than a week or two beforehand the fresh system is installed. This is because majority of the individuals usually do not recall what they learned in the training meetings. The study nevertheless did not triangulate to get the opinions of high-ranking bosses.

### **2.5.3 Complexity of Information Systems**

Comparative advantages together with complexity ones are recognized as characteristics that impact a probable adopter concerning security systems of information adoption. According to Thong (2016), relative advantage is the benefit added from embracing an invention. As per a study on the adoption of Picture Archiving and Communication Systems done in the Taiwan healthcare sector, adopters together with non-adopters settled that the healthcare sector in Taiwan is competitive. As per Hung et al. (2015), adopters of data security of information systems inclines to use them as an instrument for amassing client satisfaction plus improving medical service quality so as to assist the hospitals achieve relative advantage together with eventually grow operation presentation.

As per Rogers's (2013) innovation theory, a person forms an attitude toward the innovation, materializing to a conclusion to accept or reject and, if the decision is to implement, to execution of the novelty. The key determinant of systems of information adoption is the perception of the potential adopter. Tornatzky and Klein (2014) founded on a meta-analysis of the technological innovation works regarding the nature of novelties, recognized relative benefit, and compatibility together with intricacy as innovation features that are noticeable to the attitude growth. Compatibility is the level to which a novelty is viewed as reliable with the



current morals, wants together with previous experiences of the potential adopter as per Rogers (2013). If the system of information is well matched with the current job practices, the small enterprises will be more probable to adopt them. According to Rogers (1983), complexity to the level to which an innovation is viewed as problematic to use. The viewed complexity of the system of information is expected to impact the decision to adopt them undesirably.

Mugeni et al (2014) as per their study on assessing factors affecting broadband implementation in Kenya stated that comparative gain of broadband worldwide web over its predecessor narrowband world wide web was very significant in clarifying disparities in broadband intention. Bearing in mind the items that are used to measure this construct, conspicuously faster download speeds, higher dependability, better value of service together with improved quality of experience, policy makers together with controllers are referred upon to foster a suitable allowing surroundings. Obtainability of a national broadband approach would in addition serve as a blueprint for broadband growth and set clear targets of download together with upload speeds, and others.

#### **2.5.4 Lack of Top Management Support**

Doolin (2014) observed that while the execution of new systems of information in firms be contended for with regard to efficacy plus rationality, the social and political pressure within the company could result in the opposite effect and all these depends on the structures put in place. Leadership is defined as the ability to influence others behavior. There is need for sustained high level ICT leadership and championship in all middle level institutions to provide oversight, inspiration and political goodwill. Effective leadership requires the mobilization of much needed resources needed to develop an ICT environment.

Dewar and Dutton (2016) in their research established that extensive knowledge is significant for the adoption of technical procedure innovations. The study has also discovered numerous executives' characteristics that affect the adoption of information/data process. As per Rogers (2013), innovation adoption is connected to innovation decision process. When the information of the innovation is collected, an attitude will be established about the innovation as if to adopt or discard innovation. Grounded on the internal needs of the company or environmental variations high ranking executives will make the ultimate decision to implement IT. A firm's strategic decision to adopt or decline an innovation often portrays the particular characteristics of its top directors. Therefore, researchers have often scrutinized numerous characteristics of CEO when addressing the issues influencing the adoption of information technology in companies.

According to Sabherwal et al., (2016), Information is comparable to blood that streams into the company's vessels and gives it life. Information security systems' purpose in executing procedures that are commonly concerned with internal flow of data plus it acts on conservational indecision phenomenon. Another vital matter that shows the part of security of information systems in executing strategy is exchange of data. Information system is one of tools that can gather together for directors to do their jobs.

## **2.6 Summary**

This section has looked into the accessible literature on information security threats, and challenges to adoption of information security systems. It has looked into predictive framework for influencing the adoption of digital security in businesses. These models demonstrate that information systems security is a must-do for Kenyan cloud based lenders in order to protect their data assets.

The study will also look at earlier research on the issue that addressed information systems in general or specific aspects of the topic in other settings than the one being investigated. The literature on current information security risks, as well as the information security systems used by these firms in Kenya and other areas of the world, was reviewed. In addition, the literature on information system security adoption was studied. This study therefore looked at this aspect - information system security - at a local perspective that is in the context of digital lending in Kenya.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.1 Introduction**

This chapter presents the methodology used namely the research design, population, together with information gathering and analysis procedures.

#### **3.2 Research Design**

Research design is the scheme or blueprint used in providing answers to the research questions (Kothari, 2007). In this study, a descriptive research design was adopted. As per Mugenda and Mugenda (2008), descriptive research designs is suitable when the researcher aims to provide basic information about variables in a dataset and highlight potential relationships between variables. The research design was descriptive in which interconnected factors were measured at an explicit point in time for a definite populace.

#### **3.3 Population**

There were 29 registered digital lenders operating in Kenya as at the time of the study. Digital lenders operating within the banking and microfinance industry were 16 while digital-first lenders operating in the Fintech industry were 13. This study targeted all 29 digital lenders operating in Kenya as at the time of the study in April 2021 .

#### **3.4 Data Collection**

This research gathered primary data using a structured questionnaire. The questionnaires consisted of closed-ended questions. Further, they were administered to the ICT managers, IT managers, Chief Information Officers (CIOs) and ICT Officers. The questionnaire was

administered using a drop-and-pick later technique for firms in close proximity and through email for those further away.

### **3.5 Data Analysis**

The collected data was sorted, checked for completeness, coded and then analyzed with IBM Statistical Package for Social Scientists (SPSS) version 25 software program. For objective 1 of the study was analyzed using mean and standard deviation. For objective 2 and for objective 3 of the study were analyzed using both mean and standard deviation and factor analysis method. Further, demographic and organizational data was analyzed using frequencies and percentages. The purpose of using factor analysis was to discover relationships among variables, in order to understand their underlying structure.

## **CHAPTER FOUR**

### **DATA ANALYSIS, RESULTS AND DISCUSSION**

#### **4.1 Introduction**

This chapter outlines data analysis, presentation and discussion of the study findings. The purpose of the study was to determine information security threats faced by digital lenders, information security measures adopted by digital lenders and establish challenges faced by digital lenders in securing their information systems.

#### **4.2 Response Rate**

A total of 29 questionnaires were administered to Kenyan digital lenders. A total of 16 questionnaires received back resulting in a 55.17% response rate. Mugenda Mugenda (2003) postulates that a response rate of 50% is acceptable for analysis and reporting. Therefore the response rate for this study was considered adequate by the researcher to make recommendations and conclusions.

#### **4.3 Demographic Characteristic of Respondents**

The research set out to determine the demographic characteristics of the 29 respondents, which included; gender, age, education qualifications, role in the respective organizations, and work experience.

##### **4.3.1 Distribution of Respondents by Age and Highest Education Level**

The participants were asked to specify their age and highest education level. Results were as displayed in Table 4.1 and 4.2.

**Table 4.1: Distribution of Respondents by Age**

Age	Frequency	Percent
26– 30 years	1	6.3
31 - 35 years	6	37.5
36 - 40 years	7	43.8
41 - 45 years	2	12.5
Total	16	100.0

**Source, Research data (2021)**

Table 4.1 exhibits that the highest proportion of the respondents were aged between 36-40 years. Respondents whose ages ranged from 31 to 35 constituted 37.5% and proportion of those aged 41-45 years were 12.5%.

**Table 4.2: Distribution of Respondents by Highest Education Level**

Education Level	Frequency	Percent
Postgraduate Degree	5	31.3
Bachelor's Degree	11	68.8
Total	16	100.0

**Source, Research data (2021)**

Table 4.2 exhibits the highest education qualifications of the study respondents. The highest proportion of the respondents had a bachelor's degree qualification while those who had postgraduate degree qualification were 31.3%.

#### **4.3.2 Distribution of Respondents by Position Held and Work Experience**

The researcher asked this question to establish position held and work experience of the respondents. The highest proportion of respondents, 37.5%, under the category called "Other" held the position of Application and Security Engineer, and Fintech Administrator.

The highest proportion of respondents had worked for their respective digital lenders for 5 years or less, which constituted 75%. The results of the role and work experience of the respondents are displayed in Table 4.3 and 4.4.

**Table 4.3: Distribution of Respondents by Position Held in their Organization**

Positions Held by Respondents	Frequency	Percent
ICT Manager	5	31.3
Chief Information Officer (CIO)	1	6.3
IT Officer	4	25.0
Other	6	37.5
Total	16	100.0

**Source, Research data (2021)**

**Table 4.4: Distribution of Respondents by Work Experience**

Work Experience	Frequency	Percent
5 years or less	12	75.0
6-10 years	2	12.5
Above 11 years	2	12.5
Total	16	100.0

**Source, Research data (2021)**

#### **4.4 Organizational Information**

The research set out to determine the years the digital lending firms had been in operation, what sector they operated in, their ownership structure, and the number of employees.

##### **4.4.1 Distribution of Respondent's Firm by Duration of Operation**

The highest proportion of the digital lenders, which constituted 37.5% each, had been in operation for 1 to 4 years and 5 to 10 years. The least proportion of the digital lenders, which constituted 25%, had been in operation for more than 10 years.



#### 4.4.2 Distribution of Respondent's Firm by Sector and Ownership Structures

The researcher asked this question to determine whether their respective digital lender operated in the banking, microfinance institution (MFI) or Fintech sector. The findings showed that the highest proportion, 50%, operated in the Fintech sector. Additionally, 31.3% of the respondents operated in the banking sector while 18.8% operated in the Microfinance Institutions (MFI) sector.

Further, the researcher asked about the ownership structures of the digital lenders. Whether they were purely foreign owned, purely locally owned, or ownership constituted of both local and foreign shareholdings. The findings in Table 4.5 showed that 56.3% of digital lenders have both local and foreign shareholdings while 43.8% were locally owned. None of the digital lenders were totally foreign owned.

**Table 4.5: Distribution of Respondent's Firm by Ownership Structures**

Ownership Structures	Frequency	Percent
Locally Owned	7	43.8
Both	9	56.3
Total	16	100.0

Source, Research data (2021)

#### 4.4.3 Distribution of Respondents by Size of Respondents Firms

Respondents were asked to specify how many employees work at the digital lending firms in which they are currently engaged in. The highest proportion of 37.5% had 49 or less employees, findings in Table 4.6. Banking and micro-finance institutions represented 31.3% of above 1000 employees and 12.5% of between 101 to 999 employees respectively. Further medium sized digital-first lenders represented 18.8% of between 50 to 100 employees.

**Table 4.6: Distribution of Respondents by Size of Respondents Firms**

Number of employees	Frequency	Percent
49 or less	6	37.5
50 to 100	3	18.8
101 to 999	2	12.5
Above 1000	5	31.3
Total	16	100.0

Source, Research data (2021)

#### 4.5 Information Security Threats Faced by Digital Lenders in Kenya

The study sought to determine the information security threats faced by digital lenders. To accomplish this objective, several information security threats were listed and the respondents were requested to indicate the extent that those threats were faced by their digital lenders. The rating was on a five-point Likert scale of 1 to 5 (1 = no extent, 2 = little extent, 3 = moderate extent, 4 = great extent and 5 = very great extent). The responses were analyzed using means and standard deviations and the study findings are presented in Table 4.7.

**Table 4.7: Rating of Information Security Threats**

Information Security Threats	Mean	Std. Deviation
1. A phishing attack where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information.	3.56	1.153
2. Potentially destructive malicious software such as Malware, Adware, Spyware and Viruses being used to collect personal information	3.19	1.721
3. A Distributed Denial of Service (DDoS) attack that has resulted in websites and servers being unavailable to legitimate users.	2.63	.957
4. Fake plug-ins posing as legitimate extensions (Trojans) that trick users to download and install them leading to infection and stealing of information from the infected machine(s)	2.56	1.548
5. A brute force attack where hackers used all possible password combinations to guess a password correctly.	2.44	1.413

6. An external breach of access to secret or confidential information stored either in the organization's computers or ICT network.	2.31	1.448
7. Employees carelessly making mistakes that compromise information security.	2.31	1.014
8. A sniffing attack where hackers obtained passwords by "sniffing" the network connection in order to gain access to passwords.	2.27	1.280
9. Employees unintentionally making mistakes that compromise information security.	2.13	.957
10. Employees being tricked by parties external to the organization to give out their security information for example passwords	2.13	1.187
11. An attack that allows someone to eavesdrop on communication between two targets also known as Man-in-the-middle.	2.13	1.025
12. Employees logging into the network to delete files and change passwords, leaving admins unable to log into switches.	1.94	1.237
13. Privileged users for example, IT administrators, attacking the organization's information system for any reason.	1.81	1.276
14. Disgruntled employees intentionally compromising information security for instance as result of being bypassed on a promotion	1.75	1.390
15. Computers in the organization used by third parties to conduct online fraud activities	1.63	1.147
16. Malfunction printers within an office environment being exposed to unauthorized access via the operator panel	1.63	1.258
17. Employees gaining unauthorized access to steal private customer information, including contacts and bank details.	1.81	1.167
18. Network engineers resetting servers to their original factory settings.	1.50	.817
19. Printer's built-in software — also known as firmware — being used as a method of intrusion into the corporate network.	1.88	1.088
20. They use malicious code (SQL injection attack) to obtain private data, change and even destroy that data in order to void transactions on websites.	1.81	1.109
21. A dictionary attack as a method used to break into a password-protected computer or server.	1.69	1.138

**Source, Research data (2021)**

The study findings presented in Table 4.7 show that the major threats to information security facing digital lenders in Kenya were phishing attacks where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information (mean = 3.56, std deviation = 1.153) and Potentially destructive malicious software such as Malware, Adware, Spyware and Viruses being used to collect personal information (mean = 3.19, std deviation=1.721).

Table 4.8, presents four factors with eigen values greater than 1. All these numbers summed up to almost 84% of the initial variable's variability. Factor 1 accounts for 51.243% of the variability in all 21 variables while factor 2 accounts for 19.086% of the variability in all 21 variables. Thus, there were four factors generated for information security threats facing digital lenders in Kenya. The Rotated Component Matrix presented in Table 4.9 showed the factor loadings for each variable. Where there was more than one factor loading indicated in the components, every variable's most heavily loaded factor was chosen.

**Table 4.8: Total Variance Rating of Information Security Threats**

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	10.761	51.243	51.243	10.761	51.243	51.243
2	4.008	19.086	70.329	4.008	19.086	70.329
3	1.774	8.448	78.778	1.774	8.448	78.778
4	1.223	5.823	84.601	1.223	5.823	84.601
5	.931	4.432	89.033			
6	.718	3.417	92.450			
7	.436	2.076	94.526			
8	.388	1.850	96.376			
9	.295	1.405	97.781			
10	.188	.896	98.677			
11	.123	.587	99.264			
12	.076	.360	99.624			
13	.049	.231	99.855			
14	.030	.145	100.000			
15	5.323E-16	2.535E-15	100.000			
16	2.705E-16	1.288E-15	100.000			
17	9.978E-17	4.751E-16	100.000			
18	-4.254E-17	-2.026E-16	100.000			
19	-1.703E-16	-8.109E-16	100.000			
20	-2.987E-16	-1.422E-15	100.000			
21	-8.036E-16	-3.827E-15	100.000			

Source, Research data (2021)

**Table 4.9: Rotated Component Matrix of Information Security Threats**

Information Security Threats	Component			
	1	2	3	4
Employees unintentionally making mistakes that compromise information security.	.744	- .383		.255
Employees carelessly making mistakes that compromise information security.	.770	- .324	.324	.185
Disgruntled employees intentionally compromising information security for instance as result of being bypassed on a promotion	.852	.103	.442	.138
Employees being tricked by parties external to the organization to give out their security information for example passwords	.675	.584		.105
Privileged users for example, IT administrators, attacking the organization's information system for any reason.	.841	.378		.188
Computers in the organization used by third parties to conduct online fraud activities	.802	.310		.208
Malfunction printers within an office environment being exposed to unauthorized access via the operator panel	.917	.183	.220	
Employees gaining unauthorized access to steal private customer information, including contacts and bank details.	.665	.620	.107	
Employees logging into the network to delete files and change passwords, leaving admins unable to log into switches.	.743	.435		.250
Network engineers resetting servers to their original factory settings.	.869		.169	.140
Fake plug-ins posing as legitimate extensions (Trojans) that trick users to download and install them leading to infection and stealing of information from the infected machine(s)	.416	.447	- .137	.629
A Distributed Denial of Service (DDoS) attack that has resulted in websites and servers being unavailable to legitimate users.	.354	.158	.212	.767
An external breach of access to secret or confidential information stored either in the organization's computers or ICT network.	.224	.838	.189	.225
Potentially destructive malicious software such as Malware, Adware, Spyware and Viruses being used to collect personal information	- .116	.712		.550
Printer's built-in software — also known as firmware — being used as a method of intrusion into the corporate network.	.305	.148	.828	.196
They use malicious code (SQL injection attack) to obtain private data, change and even destroy that data in order to void transactions on websites.	.808		.513	
An attack that allows someone to eavesdrop on communication between two targets also known as Man-in-the-middle.	.142	.285	.872	
A dictionary attack as a method used to break into a password-protected computer or server.	.680	.163	.532	- .248
A brute force attack where hackers used all possible password combinations to guess a password correctly.		.939		.179

A sniffing attack where hackers obtained passwords by “sniffing” the network connection in order to gain access to passwords.	.238	.808	.428	
A phishing attack where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information.		.652	.192	.617
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.				
a. Rotation converged in 9 iterations.				

**Source, Research data (2021)**

The following section discuss statements under each of the factors

Factor 1

- A dictionary attack as a method used to break into a password-protected computer or server.
- They use malicious code (SQL injection attack) to obtain private data, change and even destroy that data in order to void transactions on websites.
- Network engineers resetting servers to their original factory settings.
- Employees accessing the network to remove files and change passwords, preventing administrators from accessing switches.
- Employees gaining unauthorized access to steal private customer information, including contacts and bank details.
- Malfunction printers within an office environment being exposed to unauthorized access via the operator panel
- Machines at the company are being utilized by third parties to commit online fraud.
- For whatever cause, privileged users, such as IT professionals, assault the company's information system.
- Employees are lured into divulging their security details, such as passwords, by third parties outside the firm.
- Disgruntled employees intentionally compromising information security for instance as result of being bypassed on a promotion

- Employees carelessly making mistakes that compromise information security.
- Lack of enough staff to take care of your information security needs

#### Factor 2

- An unauthorized outsider gaining access to special or private data housed on the agency's machines or ICT network.
- Potentially destructive malicious software such as Malware, Adware, Spyware and Viruses being used to collect personal information
- A brute force attack where hackers used all possible password combinations to guess a password correctly.
- A sniffing attack where hackers obtained passwords by “sniffing” the network connection in order to gain access to passwords.
- A phishing attack where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information.

#### Factor 3

- Printer's built-in software — also known as firmware — being used as a method of intrusion into the corporate network.
- An attack that allows someone to eavesdrop on communication between two targets also known as Man-in-the-middle.

#### Factor 4

- Trojans (fake plug-ins masquerading as legal extensions) that fool users into downloading and installing them, resulting in infection and data theft from the afflicted PC (s)
- A decentralized disruption of access (DDoS) assault that caused genuine users to be unable to access websites and services.

Factor 1 can be summarized as *Internal Information Security Threats*. A significant number of internal threats are caused by employees' leading to intentional or unintentional harm to information systems. IS systems are operated by individuals. If one of those trusted individuals chooses to break the trust it can be problematic to forecast or stop (Shelley, 2015).

Factor 2 can be summarized as *External Information Security Threats*. External threat actors include hackers or advanced persistent threats that are skilled and determined to break into systems for economic gain (SentinelOne, 2019). External threats to IS can originate from anywhere and may take on many forms such as social engineering attacks, DDoS attacks, malware, spyware, adware or viruses.

Factor 3 can be summarized as *Inherent Hardware Vulnerabilities*. When inherent vulnerabilities exist in an IS such as a Zero day attack, there is a potential risk of exploitation (Watts, 2020).

Factor 4 can be summarized as *Social Engineering Attacks*. The goal of social engineering assault is to trick people on the target website into exposing personal or sensitive information. One of the components that loaded was bogus plug-ins masquerading as real extensions (Trojans), which were used to deceive users into downloading and installing them, resulting in infection and data theft from the compromised PC(s).

The findings from the analysis presented reaffirms that the major threat to information security that are faced by digital lenders was phishing attacks where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information (mean = 3.56, std deviation = 1.153)



#### 4.6 Information Security Measures Adopted by Digital Lenders in Kenya

The study sought to determine the information security measures adopted by digital lenders in Kenya. To accomplish this objective, several information measures were listed and the respondents were requested to indicate the extent that those threats were faced by their digital lenders. The rating was on a five-point Likert scale of 1 to 5 (1 = no extent, 2 = little extent, 3 = moderate extent, 4 = great extent and 5 = very great extent). The responses were analyzed using means and standard deviations and the study findings are presented in Table 4.10.

**Table 4.10 Rating of Information Security Measures Adopted**

<b>Information Security Measures Adopted</b>	<b>Mean</b>	<b>Std. Deviation</b>
1. Automatic logout policy for workstations after a predetermined period of inactivity.	4.75	.577
2. Password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols.	4.75	.447
3. Firewalls are used to provide a secure barrier among both your network or an active layer like the internet.	4.63	.719
4. Permission based access control as a method used to restrict access sensitive resources.	4.50	.894
5. Password preservation policy that limits the number of times an old password may be used, deterring users from doing so.	4.38	1.088
6. Regular information risk assessments conducted on critical assets as a way of determining existing vulnerabilities in systems.	3.69	1.078
7. Users are discouraged from using outdated passwords by a password retention policy that restricts the handful of times they may be used.	4.00	1.095
8. A controls policy that defines control and operational modes such as fail secure, fail open, allowed unless specifically denied and denied unless specifically permitted.	4.00	1.211
9. As a fundamental internal control that prevents and identifies mistakes, segregation of responsibilities is used.	4.25	1.183
10. The optimum username age policy establishes how part of generation must maintain a credential already when it must be changed.	4.13	1.302
11. Port blocking policy that selectively blocks ports from sending or receiving data.	3.50	1.265

**Source, Research data (2021)**

The study findings presented in Table 4.10 show that information security measures adopted by digital lenders included automatic logout policy for workstations after a predetermined

period of inactivity (mean = 4.75, std deviation = 0.577), password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols (mean = 4.75, std deviation = 0.447), and application of firewalls that enforce a secure boundary between your internal network and an open environment such as the internet (mean = 4.63, std deviation = 0.719).

Only values with eigen values larger than one were kept after the factor analysis. As a result, five components had eigen values larger than one. All of these numbers added up to about 80% of the variability in the initial variable. The "percentage of variance" column displays how much of the overall variability in all of the variables can be explained by each of the components extracted individually. As shown in Table 4.11, factor 1 is responsible for 31.696 percent of the variance in all 17 variables, whereas factor 2 is responsible for 17.037 percent of the variance in all 17 variables.

**Table 4.11 Total Variance Rating of Information Security Measures Adopted**

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.388	31.696	31.696	5.388	31.696	31.696
2	2.896	17.037	48.733	2.896	17.037	48.733
3	2.451	14.416	63.149	2.451	14.416	63.149
4	1.860	10.942	74.091	1.860	10.942	74.091
5	1.160	6.824	80.915	1.160	6.824	80.915
6	.829	4.877	85.792			
7	.785	4.620	90.411			
8	.598	3.519	93.930			
9	.402	2.365	96.295			
10	.274	1.613	97.908			
11	.142	.835	98.743			
12	.131	.769	99.512			
13	.059	.347	99.859			
14	.024	.141	100.000			
15	7.242E-16	4.260E-15	100.000			
16	1.683E-16	9.902E-16	100.000			
17	-6.592E-17	-3.878E-16	100.000			

Source, Research data (2021)

Finally, the Rotated Component Matrix in Table 4.12 was generated, it showed the each variable's factor loadings. The factor on which each variable had the greatest impact is displayed. Where there is more than one factor loading indicated in the components, each variable's most heavily loaded factor was chosen.

**Table 4.12: Rotated Component Matrix of Information Security Measures Adopted**

	Component				
	1	2	3	4	5
An Information System Security (ISS) Policy	.584	.684	.134		
The use of Two-factor authentication as a user access control mechanism aimed at achieving confidentiality of resources	- .163	.868			- .197
The use of continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs)	.594	.478		.132	.474
Permission based access control as a method used to restrict access sensitive resources.		.317	.719	- .331	.335
Adoption of user awareness training for all employees on information security issues	.354	.284	.697		- .163
Application of encryption protocols such as HTTPS as a means of securely transmitting data over the internet.	- .122	.905	.216		.158
Regular information risk assessments conducted on critical assets as a way of determining existing vulnerabilities in systems.	.836	.231		.143	- .348
Content filtering as a means of controlling access to a network by analyzing the contents of incoming and outgoing packets.	.217	.170	.872		
A controls policy that defines control and operational modes such as fail secure, fail open, allowed unless specifically denied and denied unless specifically permitted.	.835		.305		- .118
Application of firewalls that enforce a secure boundary between your internal network and an open environment such as the internet.	.375	.575			.386
Segregation of duties as a basic internal control that prevents and detects errors.	.815			- .496	.200
Maximum password age policy that determines how long users must keep a password before they are required to change it.	.815	- .148		- .297	
Password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols.			.435	.663	.186

Password history policy that sets how often an old password can be reused discouraging users from reusing an old password.		- .305	.823	.162	- .131
Account lockout policy that locks out users after a defined number of failed password attempts.	- .130			.863	.130
Automatic logout policy for workstations after a predetermined period of inactivity.			- .144	.434	.774
Port blocking policy that selectively blocks ports from sending or receiving data.	.731	- .232	.336		.311
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.					
a. Rotation converged in 23 iterations.					

**Source, Research data (2021)**

The following section discuss statements under each of the factors

Factor 1

- An Information System Security (ISS) Policy
- Through use of ongoing network activity demand side management ( dsm on gateways and file systems (CPUs)
- Regular information risk assessments conducted on critical assets as a way of determining existing vulnerabilities in systems.
- A controls policy that defines control and operational modes such as fail secure, fail open, allowed unless specifically denied and denied unless specifically permitted.
- By evaluating the contents of receiving and sending packets, utilization of data may be used to regulate network access
- Firewalls are used to provide a secure barrier between company company's network and an opportunity to move like the internet.
- Port blocking policy that selectively blocks ports from sending or receiving data.

Factor 2

- The use of Two-factor authentication as a user access control mechanism aimed at achieving confidentiality of resources
- Application of encryption protocols such as HTTPS as a means of securely transmitting data over the internet.
- The limit password age policy establishes how part of generation must maintain a credential before it will be changed. Factor 3
- Password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols.
- Account lockout policy that locks out users after a defined number of failed password attempts.

#### Factor 4

- Automatic logout policy for workstations after a predetermined period of inactivity.

From the results, factor 1 can be summarized as *Information System Security Policies*. Security controls, as per Briffa (2020), are the "legislature" of security controls and so must be clearly connected with and support the organization's strategic security objectives. This might explain why Kenyan Digital Borrowers have implemented regulations as an IT governance and compliance tool.

Factor 2 can be summarized as *Information security access controls*. Security controls are a way of managing risk which can be of an administrative, technical, management or legal nature. It reveals Digital Lenders in Kenya have adopted access controls as a means to directly reduce vulnerabilities and threats in their computing environment.

Factor 3 may be summed up as *Knowledge of Information Security*. People provide the biggest threat to every company, whether through accident, error, ignorance, or intentional purpose. Appropriate awareness and education may make a big difference when it comes to reducing information security threats. As a result, it has been discovered that Kenyan Digital Lenders

have implemented information security awareness training for their employees in order to combat rising dangers.

Password regulations may be summed up as factor number four. Learning the username and password of an authorized system user is one of the most basic ways used by attackers to obtain unauthorized access to a system. They'll have a footing in the system after they've acquired access. As a result, it explains why Kenyan Digital Lenders have implemented password policies to remind users of the necessity of choosing a safe password and keeping it secret.

Finally, Factor 5 can be summarized as *Logout Policy for Workstations*. This is a workstation security policy adopted to include automatic logoff procedures, limiting accidental disclosure of personal identifiable information.

The findings from the analysis presented reaffirms that to a very great extent there were three major information security measures adopted by digital lenders. These were automatic logout policy for workstations after a predetermined period of inactivity (mean = 4.75, std. deviation = 0.577), password complexity requirements policy to ensure every password met minimum required threshold of length, characters, numbers and symbols (mean = 4.75, std. deviation = 0.447), and application of firewalls that enforce a secure boundary between your internal network and an open environment such as the internet (mean = 4.63, std. deviation = 0.719).

#### **4.7 Challeges Faced by Digital Lenders in Securing their Information Systems**

The study sought to determine the challenges faced by digital lenders in Kenya in securing their information systems. To accomplish this objective, several challenges were listed and the respondents were requested to indicate the extent that those threats were faced by their digital lenders. The rating was on a five-point Likert scale of 1 to 5 (1 = no extent, 2 = little extent, 3 = moderate extent, 4 = great extent and 5 = very great extent).

The responses were analyzed using means and standard deviations and the study findings are presented in Table 4.13.

**Table 4.13: Rating of Information Security Challenges**

<b>Information Security Challenges</b>	<b>Mean</b>	<b>Std. Deviation</b>
1. Lack of awareness by customers on the risk of sharing their passwords	3.81	1.047
2. Lack of information security awareness amongst customers.	3.81	1.047
3. Lack of information security awareness amongst partners.	3.38	1.204
4. Lack of information security awareness amongst employees	3.00	.894
5. Lack of awareness amongst employees of social engineering attacks aimed at gaining access to confidential data.	3.25	1.342
6. Lack of awareness amongst employees of phishing attacks where hackers copy the image of sites almost perfectly with the aim of stealing their passwords.	3.31	1.401
7. Lack of awareness amongst employees of phishing attacks where hackers copy the image of sites almost perfectly with the aim of stealing their passwords.	3.31	1.401
8. Lack of awareness amongst employees on the risk of sharing their passwords.	2.87	1.506
9. Lack of additional security, such as decryption, for personal data in transit or at rest.	2.50	1.211
10. Limited visibility within your IT environment resulting in not being able to fix and manage what you are not aware of.	2.69	.946
11. The information security strategy not being aligned with the overall business goals	2.13	1.088
12. Security misconfigurations that are as a result of insecure default configurations.	2.19	.981
13. Insufficient logging and monitoring that allow hackers to further attack systems.	2.19	1.109
14. Incorrect implementation of authentication management that allow attackers to compromise passwords.	2.19	1.185
15. Bridge scripting issues are present, allowing intruders to takeover data traffic, deface services, and divert contain malware websites.	2.19	1.167
16. Lack of regular automated running of antivirus checks on workstations	2.19	1.377

**Source, Research data (2021)**

The study findings presented in Table 4.13 show that challenges faced by digital lenders in securing their information systems included lack of awareness by customers on the risk of

sharing their passwords (mean = 3.81, std deviation = 1.047) and lack of information security awareness amongst customers (mean = 3.81, std deviation = 1.047).

Table 4.14 presented that there were eight factors with eigen values greater than 1. All these values summed up to almost 92% of the initial variable's variability. Thus, there were eight factors generated for challenges faced by digital lenders in securing their information systems. Factor 1 accounts for 29.116% of the variability in all 24 variables while factor 2 accounts for 24.823% of the variability in all 24 variables.

**Table 4.14: Total Variance Rating of Information Security Challenges**

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.988	29.116	29.116	6.988	29.116	29.116
2	5.958	24.823	53.939	5.958	24.823	53.939
3	2.220	9.249	63.188	2.220	9.249	63.188
4	2.041	8.504	71.692	2.041	8.504	71.692
5	1.676	6.983	78.674	1.676	6.983	78.674
6	1.281	5.338	84.012	1.281	5.338	84.012
7	1.083	4.514	88.526	1.083	4.514	88.526
8	1.058	4.410	92.936	1.058	4.410	92.936
9	.645	2.687	95.623			
10	.409	1.704	97.327			
11	.331	1.379	98.706			
12	.176	.732	99.438			
13	.072	.298	99.736			
14	.063	.264	100.000			
15	4.580E-16	1.909E-15	100.000			
16	2.332E-16	9.717E-16	100.000			
17	2.084E-16	8.685E-16	100.000			
18	3.893E-17	1.622E-16	100.000			
19	-6.933E-18	-2.889E-17	100.000			



20	-1.318E-16	-5.490E-16	100.000			
21	-2.870E-16	-1.196E-15	100.000			
22	-5.402E-16	-2.251E-15	100.000			
23	-8.483E-16	-3.535E-15	100.000			
24	-1.718E-15	-7.158E-15	100.000			

**Source, Research data (2021)**

The Rotated Component Matrix in Table 4.15 showed the factor loadings for each variable. Where there was more than one factor loading indicated in the components, the factor that each variable loaded most strongly on was picked

**Table 4.15: Rotated Component Matrix of Information Security Challenges**

	Component							
	1	2	3	4	5	6	7	8
Inadequate support from top management on issues regarding information security.			.133	.866		.258		
Lack of staff ICT skills as an obstacle to implementation of information security control measures.	-.109		.168	.863	.186	-.164	.152	.162
Budgetary constraints for Information Security infrastructure	.254	.794	-.170				.245	-.414
Lack of expertise within the organization in managing information security issues		.143		.170	.919	-.172		
Lack of information security enforcement and accountability procedures	.193				-.260		.869	-.105
Lack of information security strategy that are clearly defined and approved by senior management	-.337	.235	.170	.387	.422		.597	.241
Lack of information goals that are clearly defined and approved by senior management.	-.224	.128	.432	.327	.257		.679	.136
Lack of enough staff to take care of your information security needs	-.500	.312		.250	.366	.377		.421

Limited visibility within your IT environment resulting in not being able to fix and manage what you are not aware of.	.293	.730	- .456	- .263	.118	.214		
The information security strategy not being aligned with the overall business goals	- .192	.114	.154	.612	.358	.264	.343	.366
Lack of information security awareness amongst employees	.618	.475	- .107		.252	.102	.354	- .158
Lack of information security awareness amongst customers.	.487		- .717		.136		- .183	- .249
Lack of information security awareness amongst partners.	.735	.299	- .451	- .197		.198		- .235
Lack of extra protection such as encryption for sensitive data at rest or in transit.	.148	.755	.387	.116	.416	.105	.147	
Security misconfigurations that are as a result of insecure default configurations.	.173	.105	.245		.711	.586	- .179	
Insufficient logging and monitoring that allow hackers to further attack systems.		.101			- .132	.964		
Incorrect implementation of authentication management that allow attackers to compromise passwords.	.316	.264	.582	.214	.201	.590		
Presence of cross-site scripting flaws that allow attackers to hijack user sessions, deface web sites, and redirect user to malicious sites.			.863	.370				.254
The use of outdated security software that allow malicious code to go undetected.		- .155	.335	.208				.874
Lack of awareness amongst employees of social engineering attacks aimed at gaining access to confidential data.	.884	.219	- .121		- .315			.186
Lack of awareness amongst employees of phishing attacks where hackers copy the image of sites almost perfectly with the aim of stealing their passwords.	.929	.262						.148

Lack of regular automated running of antivirus checks on workstations	.323	.756	.347	.256		.122		.189
Lack of awareness amongst employees on the risk of sharing their passwords.	.890				.330		.106	- .206
Lack of awareness by customers on the risk of sharing their passwords	.856	.141					- .204	- .214
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.								
a. Rotation converged in 10 iterations.								

**Source, Research data (2021)**

The following section discuss statements under each of the factors

Factor 1

- Lack of awareness by customers on the risk of sharing their passwords
- Lack of awareness amongst employees on the risk of sharing their passwords.
- Lack of awareness amongst employees of phishing attacks where hackers copy the image of sites almost perfectly with the aim of stealing their passwords.
- Lack of awareness amongst employees of social engineering attacks aimed at gaining access to confidential data.
- Lack of information security awareness amongst partners.
- Lack of information security awareness amongst customers.
- Lack of information security awareness amongst employees

Factor 2

- Budgetary constraints for Information Security infrastructure
- Limited visibility within your IT environment resulting in not being able to fix and manage what you are not aware of.
- Lack of extra protection such as encryption for sensitive data at rest or in transit.
- Lack of regular automated running of antivirus checks on workstations

### Factor 3

- Presence of cross-site scripting flaws that allow attackers to hijack user sessions, deface web sites, and redirect user to malicious sites.

### Factor 4

- Inadequate support from top management on issues regarding information security.
- Lack of staff ICT skills as an obstacle to implementation of information security control measures.
- The information security strategy not being aligned with the overall business goals

### Factor 5

- Security misconfigurations that are as a result of insecure default configurations.
- Lack of expertise within the organization in managing information security issues

### Factor 6

- Incorrect implementation of authentication management that allow attackers to compromise passwords.
- Insufficient logging and monitoring that allow hackers to further attack systems.

### Factor 7

- Lack of information security enforcement and accountability procedures
- Lack of information security strategy that are clearly defined and approved by senior management
- Lack of information goals that are clearly defined and approved by senior management.

### Factor 8

- Lack of enough staff to take care of your information security needs
- The use of outdated security software that allow malicious code to go undetected.

Factor 1 can be summarized as *Lack of Continuous Information Security Awareness*. Information security and education programs may help to ensure that everyone in the business understands how vital security is. It's a strong instrument for shaping an organization's culture, defining ethics, and influencing employee behavior. As a result, it seems that employees at

Kenyan digital lending organizations were unaware of security rules and standards, even when they were in place.

Factor 2 can be summarized as *Financial constraints*. According to Ravichandarani (2016) unsuccessful MIS executions included factors like cost overruns, missed time limit, imprecise features together with out-and-out failure. Digital lending firms in Kenya particularly the small ones cannot risk adopting costly or expensive information security systems of which they are not convinced of their advantage.

Factor 3 can be interpreted as *Risk of recurrence*. The risk that remains after management has applied risk mitigation measures is referred to as residual risk. It indicates, that Digital lending firms in Kenya may have accepted the risks after evaluation showed they were within acceptable limits.

Factor 4 can be summarized as *Inadequate support from top management*. The domain of information security systems presents a strategic problem that remains a challenge for most senior managers (Clarke, 2012). Senior manager's lack of full cooperation continues down, resulting in insufficient support from big businesses and senior staff of Kenyan digital lending enterprises.

Factor 5 can be summarized as *Lack of expertise within the organization in managing information security issues*. As an outcome, it indicates lack of adequate expertise in information security issues is a key concern for digital lending firms in Kenya. For a majority they opt to develop information security skills in-house achieved through training.

Factor 6 can be summarized as *Information Security misconfigurations*. Misconfigurations of information security architecture leads to exposure to threat actors causing significant harm and leading to data leakage.

Factor 7 can be summarized as *Lack of an information security strategies that are clearly defined and approved by senior management*. An information security plan is required to successfully meet the ever-increasing issues of providing appropriate protection for information assets. The top management of Kenya's digital lending enterprises defined the direction and goals for the information security program, which are documented in this strategy.

Factor 8 can be summarized as *Advanced Persistent Threats*. These are threats with advanced levels of knowledge and large resources, allowing them to generate chances to fulfill their goals through a variety of means. The root cause of Advanced Persistent Threats may be due to use of outdated software or lack of enough information security professionals to detect them.

The findings from the analysis presented reaffirms to a very great extent there were two major challenges facing digital lenders in Kenya in securing their information systems. These were lack of awareness by customers on the risk of sharing their passwords (mean = 3.81, std deviation = 1.047) and lack of information security awareness amongst customers (mean = 3.81, std deviation = 1.047).

#### **4.8 Discussion of Findings**

The current study revealed that there were three major information security measures adopted by digital lenders in Kenya; automatic logout policy for workstations after a predetermined

period of inactivity, password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols and lastly application of firewalls that enforce a secure boundary between the internal network and the internet. These findings confirm Rainey (2015) assertions that information security countermeasures are essentially a set of guidelines, processes, strategies, practices or governmental arrangements used for safeguarding information systems. Information security is therefore aimed at protecting information from threats through use of suitable controls. The study has shown that, to achieve reasonable assurance in information security appropriate counter measures such as policies together with user access controls can be applied.

The study further revealed that the major information security threats faced by digital lenders were phishing attacks where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information. These findings are not in agreement with Shelley (2015) that a significant number of internal threats are caused by employees' leading to intentional or unintentional harm. IS systems have trusted individuals, if one of those trusted individuals chooses to break the trust it can be problematic to forecast or stop. The study showed that the extent of an organizations exposure ought to be out in mind as it affects the likelihood that susceptibility will be exploited. When vulnerabilities exist in an IS there is a potential risk of external threat exploitation (Watts, 2020). The study also mirrors SentinelOne (2019) conclusion that external threats to IS can originate from anywhere and may take on many forms such as social engineering attacks.

The current study revealed that there were two major challenges faced by digital lenders in Kenya in securing their information systems, which were; lack of awareness by customers on the risk of sharing their passwords and lack of information security awareness amongst

customers. These findings are in agreement with Barki et al., (2015) about MIS implementation that absence of proficiency, expertise, application specific knowledge together with nonexistence of user knowledge on information system adds to MIS development threat. There is need therefore for each organization to position itself at a good information literacy level for it to identify what information is relevant or irrelevant to their business dealings. The findings espouse SentinelOne (2019) that external threat actors include hackers or advanced persistent threats that are skilled and determined to break into systems for economic purposes.



## CHAPTER FIVE

### SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

#### 5.1 Introduction

This section presents the study key findings, conclusion and recommendations. Additionally, the research limitations and further research suggestions are also outlined.

#### 5.2 Summary

The overall aim of this research was to establish adoption of information system security among digital lenders in Kenya. This research specifically sought to determine information security threats faced by digital lenders, determine information security measures adopted by digital lenders and establish challenges faced by digital lenders in securing their information systems.

This was a descriptive study which applied both mean and standard deviation and factor analysis method. There were 16 out of 29 questionnaires submitted back as responses representing 55.17% response rate. The study findings revealed that the major information security threat faced by digital lenders is phishing attacks where hackers send emails to employees that appeared to be from a trusted source in order to obtain personal information. Further findings revealed that three major information security measures adopted by digital lenders in Kenya were automatic logout policy for workstations after a predetermined period of inactivity; password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols; and application of firewalls that enforce a secure boundary between the internal network and the internet. The study findings revealed that there are two major challenges facing by digital lenders in Kenya

in securing their information systems, which were; lack of awareness by customers on the risk of sharing their passwords and lack of information security awareness amongst customers.

### **5.3 Conclusion**

The study concludes that phishing attacks where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information is the major threat facing digital lenders in Kenya. Further conclusions were that automatic logout policy for workstations after a predetermined period of inactivity, password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols and application of firewalls that enforce a secure boundary between the internal network and the internet are the major information security measures adopted by digital lenders in Kenya. The study concludes that lack of awareness by customers on the risk of sharing their passwords and lack of information security awareness amongst customers are the main challenges faced by digital lenders in Kenya in securing their information systems.

### **5.4 Recommendations**

The study recommends further researches to be carried on the field of information systems security and digital lending. It further recommends to digital lenders to create internal policies to mitigate against lack of awareness by customers on the risk of sharing their passwords and the general lack of information security awareness amongst their customers. Finally the study recommends to digital lending practitioners and consultants to enforce a secure boundary between the internal network and the internet as the information security measures to implement.

### **5.5 Recommendations for Further Study**

Exploring the field of information systems security and digital lending is crucial for policymakers in the digital lending business, as well as practitioners and "consultants." However, the current study was conducted in the digital lending industry context, and a similar study may be conducted in the healthcare or insurance industry to see if the findings hold true. The study was only done in Kenya; however, further studies can be undertaken outside of Kenya, in African or worldwide jurisdictions, to determine whether the research findings are valid.

This study used primary data, a subsequent research should be undertaken applying secondary data. The study used factor analysis; however, other analysis techniques such as principal component analysis, multiple regressions, co integration, multivariate regression, and reliability test might be used in future studies.

### **5.6 Limitations of the Study**

Due to time and expense restrictions, this study was limited to the Kenyan digital lending market. If comparable research were replicated in different countries, new conclusions would emerge. Despite the fact that the research mostly used questionnaires to collect primary data, considerable problems such as non-responsiveness of respondents were faced.

## REFERENCES

- Al-Mashari, M. & Zairi, M. (2013) Supply-chain re-engineering using enterprise resource planning (ERP) systems: An analysis of a SAP R/3 implementation case. *International Journal of Physical Distribution & Logistics Management*, 30 (3/4), 296–313.
- Abdel-Fatah, H. T. M. (2010). ISO/IEC 17025 Accreditation: between the desired gains and the reality. *The Quality Assurance Journal* , 13 (1–2), 21–27.
- Bakos, J. Y., & Brynjolfsson, E. (2005). Information technology, incentives, and the optimal number of suppliers. *Journal of Management Information Systems*, 10(2), 37–53.
- Barki, H., Rivard, S. & Talbot, J. (2015). Toward an assessment of software development risk. *Journal of Management Information Security Systems*, 10(2), 203–25.
- Benaroch, M. & Appari, A. (2010). Financial pricing of software development risks, IEEE Software, 65-73. *International Journal of Internet and Enterprise Management*, 6(4), 297-314.
- Briffa, K. (2020, October 1). *The importance of having an IT security policy in place*. Retrieved August 18, 2021
- Brandin, B., Malik, R., & Malik, P. (2004). Incremental verification and synthesis of discrete-event systems guided by counter examples. *IEEE transactions on control systems technology*, 12(3), 387–401. <https://doi.org/10.1109/tcst.2004.824795>
- Chan, S. L. (2011) Information technology in business processes. *Business Process Management Journal*, 6 (3), 224–237.
- Cooper, D. R., & Schindler, P. S. (2014). *Business research methods* (10<sup>th</sup>ed.). New Delhi: Tata McGraw-Hill Publishing Company Limited.
- Cyber Security Overview. (2018, July 13). *Communications Authority of Kenya*.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319. <https://doi.org/10.2307/249008>

- Didenko, A. (2017). Regulatory challenges underlying Fintech in Kenya and South Africa. *British Institute of International and Comparative Law*.
- Doolin, B (2014). Power and resistance in implementation of management information security systems. *Information Security Systems Journal*, 14(4), 300-340.
- Ewusi-Mensah, K. (2015). Critical issues in abandoned information security systems development projects. *Business Process Management Journal*, 7(5), 374- 386.
- Felt, A. P., Greenwood, K., & Wagner, D. (2011). The effectiveness of application permissions. *WebApps'11*
- Francis, E., Blumenstock, J., & Robinson, J. (2017). Digital credit: A snapshot of the current landscape and open research questions. *CEGA White Paper*.
- Finne, T. (1998). A conceptual framework for information security management. *Computers & security*, 17(4), 303–307. [https://doi.org/10.1016/s0167-4048\(98\)80010-2](https://doi.org/10.1016/s0167-4048(98)80010-2)
- Francis, E., Blumenstock, J., & Robinson, J. (2017). *Digital credit: A snapshot of the current landscape and open research questions*. 19.
- FSDK. (2018). Factors influencing the demand for credit by the private sector in Kenya. (2016). *European Scientific Journal*, 12(16).
- Gargeya, V. B. & Brady, C. (2015). Success and failure factors of adopting SAP in ERP system implementation. *Business Process Management Journal*, 11 (5), 501–516.
- Gibbard, M. (2005). Book Reviews Allan Gibbard, . Thinking how to live. cambridge, mass.: Harvard University Press, 2003. Pp. 302. \$45.00 (cloth). *Ethics*, 115(2), 406–412.
- Gibbs, E. L., & Gibbs, F. A. (1975). Steady spiking in the electroencephalograms of acutely ill patients. *Clinical electroencephalography*, 6(4), 191–200.
- Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2003). An integrated system theory of information security management. *Information management & computer security*, 11(5), 243–248.

- Hayikader, S., Hadi, F. N., & Ibrahim, J. (2016). Issues and security measures of mobile banking Apps. *International Journal of Scientific and Research Publications*, 6(1), 36-41.
- Kitheka, P. M. (2013). Information security management systems in public universities in Kenya: A gap analysis between common practices and industry best practices. Nairobi: (Masters Dissertation, University of Nairobi.)
- Ngalyuka, C. (2013). The relationship between ICT utilization and fraud losses in commercial banks in Kenya. Nairobi: (Masters Dissertation, University of Nairobi.)
- Nance, R. D., Worsley, T. R., & Moody, J. B. (1988). The supercontinent cycle. *Scientific American*, 259(1), 72–79. <https://doi.org/10.1038/scientificamerican0788-72>
- Hevner, A. R., March, S. T., Park, J. & Ram, S. (2014) *Design science in information system research. MIS Quarterly*, 28 (1), 75–105.
- Hong, K. K. & Kim, Y. G. (2012) The critical success factors for ERP implementation: an organizational fit perspective. *Information & management*, 40, 25–40.
- Hwang, B. H., & Tellez, C. (2016). The proliferation of digital credit deployments.
- Kaffenberger, M., & Chege, P. (2016). Digital credit in Kenya: Time for celebration or concern? *CGAP. October*, 3.
- Kaur, A., & Kumari, S. (2014). Secure database encryption in web applications. *International Journal Of Advanced Research in Computer and Communication Engineering*, 3(7), 7606-7608.
- Keil, M. Cule, P.E, Lyytinen, K. and Schmidt, R.C. (2017). A framework for identifying software project risks. *Communications of the ACM*, 41(11). 76-83
- Kroenke, D. M. (2017) *Using MIS* (2nd ed.). Upper Saddle River, New Jersey, Pearson Prentice Hall.

- Kashangaki, J. (2020, November 26). *Digital Credit – The most pressing problem in Kenyan credit markets – Really?* FSD Kenya.
- Kothari, C., & Garg, G. (2004). *Research methodology methods & techniques*. Delhi: New age international.
- Kumar, P., & Lee, H. J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1), 55–91.
- McLaughlin, M. D., & Gogan, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, 17(3), 12.
- Mengke, Y., Xiaoguang, Z., Jianqiu, Z., & Jianjian, X. (2016). Challenges and solutions of information security issues in the age of big data. *China Communications*, 13(3), 193-202.
- Milis, K. & Mercken, R. (2013) Success factors regarding the implementation of ICT investment projects. *International Journal Of Production Economics*, 80, 105–117.
- Murthy, C. S. V. (2016) *Management information security systems*. Mumbai, Himalaya Publishing House.
- Muhati, G. L., Olago, D., & Olaka, L. (2018). Participatory scenario development process in addressing potential impacts of anthropogenic activities on the ecosystem services of Mt. Marsabit forest, Kenya. *Global Ecology and Conservation*, 14, e00402.
- Mugenda, A & Mugenda, O. (2009). *Research methods: Quantitative and qualitative approaches*. Acts Press. Nairobi, Kenya.
- Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial center. *Journal of Financial Regulation and Compliance*.
- Njiru, S. W. (2013). *A framework to guide information security initiatives for banking information systems, Kenyan banking sector case study*. Nairobi.

- Nagin, D. (1978). Crime rates, sanction levels, and constraints on prison population. *Law & Society Review*, 12(3), 341. <https://doi.org/10.2307/3053284>
- Nyawira, S., Hartmann, G., Nduru, G., & Dannenberg, P. (2020). Digital connectivity at the upstream end of value chains: A dynamic perspective on smartphone adoption amongst horticultural smallholders in Kenya. *Competition & Change*, 25(2), 167–189.
- N.I.S.T. (2011, September 17). *SP 800–30 Rev. 1, Guide for conducting risk assessments / csrc*. NIST. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
- Oinas-Kukkonen, H., & Harjumaa, M. (2009). Persuasive systems design: Key issues, process model, and system features. *Communications of the Association for Information Systems*, 24.
- Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. CRC Press.
- Rajagopal, P. (2012) An innovation-diffusion view of implementation of enterprise resource planning (ERP) systems and development of a research model. *Information & Management*, 40, 87–114.
- Rodrigues (2015), International trends on hospital information security systems health strategies, Bethesda MD, USA
- Rainey, J. (2015). Preventative Control— A dynamic perspective on smartphone adoption amongst horticultural smallholders in Kenya. *Competition & Change*, 25(2), 167–189.
- Rao, R., & Herath, T. (2009). Protection motivation and deterrence: *A framework for security policy compliance in organizations* 12(1), 55–91.
- Rudolph, K. D. (2002). Gender differences in emotional responses to interpersonal stress during adolescence. *Journal of Adolescent Health*, 30(4), 3–13.
- Sabherwal, R., Jeyaraj, A. & Chowa, C., (2016). Information security systems success: Individual and organizational determinants. *Management Science* 52(12), 1849–1864



- Schmandt, J., Wilson, R., Smith, S. E., & Muller, B. H. (2019). *Promoting high technology industry: Initiatives and policies for state governments*. Routledge.
- Singh, A., & Jauhari, U. (2012). Data security by preprocessing the text with secret hiding. *Advanced computing: An nternational journal*, 3(3), 63-74.
- Soofi, A. A., Khan, M., & Fazal-e-Amin. (2014). Encryption techniques for cloud data confidentiality. *International journal of grid distribution computing*, 7(4), 11- 20.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal Of Information Management*, 36(2), 215-225.
- Spalding, J. O. (2012) Transportation industry takes the right-of-way in the supply chain. *ILE Solutons*, 30 (7), 24–28.
- Spathis, C. & Constantinides, S. (2013) The usefulness of ERP systems for effective management. *Industrial management & data systems*, 103 (9), 677–685.
- SentinelOne. (2019, September 9). Threat actor basics: Understanding the 5 main threat types. *International Journal of Production Economics*, 80, 105–117.
- Shelley, V. (2015, June 8). It's a matter of trust: protecting against insider threats. *The Quality Assurance Journal*, 13
- Theiruf, R. J. (2010) Effective management and evaluation of information technology. New York, Quorum Books.
- Totolo, E. (2018). The digital credit revolution in Kenya: An assessment of market demand, 5 years on. *FSD Kenya*. Accessed on August, 10, 2019.
- Tripathi, K. P. (2011) Role of management information system (MIS) in human resource. *International Journal of Computer Science and Technology*, 2 (1), 58–62.
- Trochim, William M.K. (2006). *Research methods knowledge base*.  
<http://www.socialresearchmethods.net/kb/scallik.php>.

- Watts, S. (2020, May 13). IT security vulnerability vs threat vs risk: What are the differences? – BMC Blogs. *International Journal of Production Economics*, 80, 105–117.
- Wimmer, B. (2015). Insider threat — an overview | science direct topics. *Industrial management & data systems*, 103 (9), 677–685
- Witt, M. T., Meek, J. W., & Beaumaster, S. (2012). Integrity and public administration. *Public integrity*, 14(3), 225–227
- Valencia-Go, J., (2015). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications; Newbury Park, CA.
- Yin, R.K. (2009). *Case study research: Design and methods*. London: Sage publications.

## APPENDICES

### Appendix I: Digital Lenders in Kenya

There are 29 registered digital lenders operating in Kenya. 16 of them operate within the banking and microfinance industry while 13 are digital-first lenders operating in the Fintech industry as listed below:

#### Digital Lenders Operating in the Banking and Microfinance Industry in Kenya

1. Bank of Africa Kenya Ltd. – Bmobile Platform	2. Credit Bank Ltd.- Connect App	3. Equity Bank Ltd.- Eazzy Loan
4. Bank of Baroda (K) Ltd. – BarodaConnect	5. Housing Finance Company of Kenya – Whizz App	6. Family Bank Limited – PesaPap Mobile
7. First Community Bank Limited – FCB Popote	8. Co-operative Bank of Kenya Ltd. – MCoop Cash	9. NCBA Bank Kenya – Mshwari
10. Kenya Commercial Bank Ltd. – KCB Mpesa	11. Prime Bank Ltd. – PrimeMobi	12. National Bank of Kenya Ltd – NatMobile App
13. SBM Bank Kenya Ltd.- Mfukoni Mobile	14. Standard Chartered Bank Kenya Ltd – SCMobile Kenya App	15. Maisha Microfinance Bank – M-Fanisi & Airtel Money Partnership
16. Okolea International Limited – Okolea Loan App		

## Digital-First Lenders Operating in the Fintech Industry in Kenya

1. Branch	2. Tala
3. Get Bucks	4. Alternative Circle
5. Stawika Capital	6. Zenka Finance
7. MyCredit	8. LPesa
9. Kopacent	10. Four Kings Investment - Sotiwa
11. Kuwazo Capital	12. Mobile Financial Solutions
13. Finance Plan Ltd	

## Appendix II: Questionnaires

### Manual questionnaire

Note: The information in this questionnaire will be treated confidentially and will not be used for any other purpose other than academic

### Section A:

#### Demographic Information

1. Gender Male [ ] Female [ ]
2. Age
  - a. 25 years or less [ ]
  - b. 26– 30 years [ ]
  - c. 31 - 35 years [ ]
  - d. 36 - 40 years [ ]
  - e. 41 - 45 years [ ]
  - f. 46 - 50 years [ ]
  - g. Over 50 years [ ]
3. What is your highest education attainment?
  - a. Postgraduate [ ]
  - b. Graduate [ ]
  - c. Diploma [ ]
4. Which of the following best represents your role in the organization?
  - a. ICT Manager [ ]
  - b. Chief Information Officer (CIO) [ ]
  - c. IT Officer [ ]
  - d. Other Specify \_\_\_\_\_
5. Length of period you have worked in the organization
  - a. 5 years or less [ ]
  - b. 6-10 years [ ]
  - c. Above 11 years [ ]

#### Organizational Information

1. For how long has your firm been in operation in Kenya?
  - a. Less than 1 years [ ]
  - b. 1 to 4 years [ ]
  - c. 5 to 10years [ ]
  - d. More than 10 years [ ]
2. In which sector does your organization operate? Tick as appropriate

- a. Banking [ ]
  - b. Microfinance Institution (MFI) [ ]
  - c. Fintech [ ]
3. Is the organization locally owned or a foreign multinational subsidiary?
- a. Locally Owned [ ]
  - b. Foreign [ ]
  - c. Both [ ]
4. Number of employees in your organization (Tick as appropriate)
- a. 49 or less [ ]
  - b. 50 to 100 [ ]
  - c. 101 to 999 [ ]
  - d. Above 1000 [ ]

**Section B: Adoption of Information Security Systems**

1. To what extent have the following information security control measures been adopted in your organization? Use a scale of 1-5 where 1= no extent, 2= little extent, 3=moderate extent, 4=great extent and 5= very great extent.

	1	2	3	4	5
An Information System Security (ISS) Policy					
The use of Two-factor authentication as a user access control mechanism aimed at achieving confidentiality of resources					
The use of continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs)					
Permission based access control as a method used to restrict access sensitive resources.					
Adoption of user awareness training for all employees on information security issues					

Application of encryption protocols such as HTTPS as a means of securely transmitting data over the internet.				
Regular information risk assessments conducted on critical assets as a way of determining existing vulnerabilities in systems.				
Content filtering as a means of controlling access to a network by analyzing the contents of incoming and outgoing packets.				
A controls policy that defines control and operational modes such as fail secure, fail open, allowed unless specifically denied and denied unless specifically permitted.				
Application of firewalls that enforce a secure boundary between your internal network and an open environment such as the internet.				
Segregation of duties as a basic internal control that prevents and detects errors.				
Maximum password age policy that determines how long users must keep a password before they are required to change it.				
Password complexity requirements policy to ensure every password meets minimum required threshold of length, characters, numbers and symbols.				
Password history policy that sets how often an old password can be reused discouraging users from reusing an old password.				
Account lockout policy that locks out users after a defined number of failed password attempts.				

Automatic logout policy for workstations after a predetermined period of inactivity.					
Port blocking policy that selectively blocks ports from sending or receiving data.					
Other: Specify and rate					

### Section C: Information Security Threats

2. To what extent have the following scenarios been experienced in your organization? Use a scale of 1-5 where 1=no extent, 2= little extent, 3=moderate extent, 4=great extent and 5= very great extent.

	1	2	3	4	5
<b>Internal Threats</b>					
Employees unintentionally making mistakes that compromise information security.					
Employees carelessly making mistakes that compromise information security.					
Disgruntled employees intentionally compromising information security for instance as result of being bypassed on a promotion					
Employees being tricked by parties external to the organization to give out their security information for example passwords					
Privileged users for example, IT administrators, attacking the organization's information system for any reason.					



Computers in the organization used by third parties to conduct online fraud activities					
Malfunction printers within an office environment being exposed to unauthorized access via the operator panel					
Employees gaining unauthorized access to steal private customer information, including contacts and bank details.					
Employees logging into the network to delete files and change passwords, leaving admins unable to log into switches.					
Network engineers resetting servers to their original factory settings.					
<b>External Threats</b>					
Fake plug-ins posing as legitimate extensions (Trojans) that trick users to download and install them leading to infection and stealing of information from the infected machine(s)					
A Distributed Denial of Service (DDoS) attack that has resulted in websites and servers being unavailable to legitimate users.					
An external breach of access to secret or confidential information stored either in the organization's computers or ICT network.					
Potentially destructive malicious software such as Malware, Adware, Spyware and Viruses being used to collect personal information					
Printer's built-in software — also known as firmware — being used as a method of intrusion into the corporate network.					

They use malicious code (SQL injection attack) to obtain private data, change and even destroy that data in order to void transactions on websites.					
An attack that allows someone to eavesdrop on communication between two targets also known as Man-in-the-middle.					
A dictionary attack as a method used to break into a password-protected computer or server.					
A brute force attack where hackers used all possible password combinations to guess a password correctly.					
A sniffing attack where hackers obtained passwords by “sniffing” the network connection in order to gain access to passwords.					
A phishing attack where hackers sent emails to employees that appeared to be from a trusted source in order to obtain personal information.					
Other: Specify and rate.					

**Section D: Challenges in Securing Information Systems**

3. To what extent have you experienced the following challenges in your organization? Use a scale of 1-5 where 1=no extents, 2= little extent, 3=moderate extent, 4=great extent and 5= very great extent.

	1	2	3	4	5
Inadequate support from top management on issues regarding information security.					

Lack of staff ICT skills as an obstacle to implementation of information security control measures.					
Budgetary constraints for Information Security infrastructure					
Lack of expertise within the organization in managing information security issues					
Lack of information security enforcement and accountability procedures					
Lack of information security strategy that are clearly defined and approved by senior management					
Lack of information goals that are clearly defined and approved by senior management.					
Lack of enough staff to take care of your information security needs					
Limited visibility within your IT environment resulting in not being able to fix and manage what you are not aware of.					
The information security strategy not being aligned with the overall business goals					
Lack of information security awareness amongst employees					
Lack of information security awareness amongst customers.					
Lack of information security awareness amongst partners.					
Lack of extra protection such as encryption for sensitive data at rest or in transit.					
Security misconfigurations that are as a result of insecure default configurations.					

Insufficient logging and monitoring that allow hackers to further attack systems.					
Incorrect implementation of authentication management that allow attackers to compromise passwords.					
Presence of cross-site scripting flaws that allow attackers to hijack user sessions, deface web sites, and redirect user to malicious sites.					
The use of outdated security software that allow malicious code to go undetected.					
Lack of awareness amongst employees of social engineering attacks aimed at gaining access to confidential data.					
Lack of awareness amongst employees of phishing attacks where hackers copy the image of sites almost perfectly with the aim of stealing their passwords.					
Lack of regular automated running of antivirus checks on workstations					
Lack of awareness amongst employees on the risk of sharing their passwords.					
Lack of awareness by customers on the risk of sharing their passwords					
Other: Specify and rate					

**THANK YOU FOR YOUR PARTICIPATION**