FRAMEWORK FOR EMERGING E-HEALTH SYSTEMS SURVIVABILITY THREATS IN KENYA: CASE OF MOI TEACHING AND REFERRAL HOSPITAL.

Simiyu Joseph Mukhwana

A Thesis submitted to the School of Computing and Informatics in Partial/fulfillment for the requirement of the Award for the degree of Master of Science in Information Technology of Masinde Muliro University of Science and Technology

October, 2024

DECLARATION

The Thesis is my original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

---------- ----------

Joseph Mukhwana Simiyu Date

SIT/G/01-53726/2019.

CERTIFICATION

The undersigned certified that they have read and hereby recommend for the acceptance of Masinde Muliro University of Science and Technology a thesis Entitled 'Framework for Emerging E-Health Systems Survivability Threats in Kenya: Case of Moi Teaching and Referral Hospital'

---------- ----------

Dr. Dorothy Rambim Date

Department of Information Technology

Masinde Muliro University of Science and Technology

---------- ----------

Dr. Jusper Ondulo Date

Department of Information Technology

Masinde Muliro University of Science and Technology

DEDICATION

This work is dedicated to my parents, Mr. Peter Sumbi Simiyu, and Mrs. Zippora Nasimiyu Simiyu, my wife Florence Adema, my children Elizabeth Wasilwa, Ashley Nasimiyu and Lloyd Tenge for giving me easy moments during my studies.

ACKNOWLEDGEMENTS

The success of this research was achieved due to the efforts and support of many, I would like to give my sincere appreciation to all Health workers and clients in Moi Teaching and Referral Hospital. This research would not have been possible without their dedication to participate. I take this opportunity to appreciate Dr. Rambim and Dr. Ondulo for their tireless effort in guidance throughout the entire Thesis supervision.

ABSTRACT

The integration of e-health presents numerous medical advantages; however, the safeguarding of these valuable data sources is inadequate. They remain vulnerable to significant threats and attacks. Moreover, the sheer volume of medical data necessitates technological solutions, yet the failure of e-health systems to prioritize security survivability renders them more susceptible to compromise. The phenomenon of remote work persists as a contemporary reality; malicious actors are probing e-health vulnerabilities to execute attacks, largely due to insufficient information security personnel and inadequate systems frameworks. The multitude of security concerns may lead the system to experience further degradation, ultimately undermining its ability to reassure users regarding their mission objectives. In spite of initiatives aimed at ensuring the resilience and security of Kenya's cyber space, ongoing attacks continue to threaten the confidentiality, credibility, reliability, and availability of e-health services for both providers and users. The emergence of e-health platforms has concurrently given rise to novel forms of crime, which are intricately linked to the advent of various modern technologies. Consequently, it is imperative that we focus on the resilience of systems in the aftermath of an attack, rather than solely concentrating on security measures. Crimes within systems are proliferating globally, and a significant number of internet users have, at some juncture, succumbed to various forms of criminal activity. Many individuals endure hardship in silence, particularly within healthcare institutions, as they are apprehensive about potential repercussions from the public. Furthermore, the risks associated with criminal activities targeting healthcare equipment and electronic healthcare technology are widespread globally, presenting significant opportunities to enhance clinical outcomes and revolutionize the provision of care. This study developed a framework for enhancing system survivability in the context of combating information systems crime within the health sector in Kenya. This research study aimed to delineate the principal threats and vulnerabilities to system survivability, formulate a framework for survivability and security, and validate its applicability for integration within the health sector in Kenya to facilitate autonomous systems. The study employed a descriptive research design. The demographic under examination Composed of personnel from the hospitals. The research concentrated on senior and mid-tier IT personnel, as well as heads of various departments within the hospital. The hospital accommodates a total of 2,056 individuals. This research employed a convenience sampling method. The study sample comprised 332 employees drawn from various departments within the hospital, as determined by the Fischer formula. Primary data was received through a structured a questionnaire. The findings were articulated through the utilization of frequency tables and percentages. Correlation and simple regression analysis were employed to elucidate the straightforward relationships between individual constructs and the dependent variable. Structural Equation Modelling (SEM) was employed for the evaluation of the framework. The research indicated that Management commitment exerted a moderate effect on System survivability ($r = .338$, $p = .000$), while organizational factors demonstrated a robust impact on system security survivability ($r = .604$, $p = .000$). Conversely, IT policies revealed a weaker influence on security and survivability ($r = .209$, $p = .028$), whereas IT literacy showed a significant effect on security and survivability ($r = .642$, $p = .000$). This research deepens understanding in the domain of information system survivability and highlights areas where knowledge is lacking, paving the way for future investigations. The research provides a deeper understanding of critical matters related to the resilience of health facilities. The research further empowers public sector policymakers to critically reassess and evaluate current security strategies, aiming to establish a robust IT-based security infrastructure for prospective applications. The research suggests that it is necessary to observe the functioning of security and survivability systems, alongside implementing ongoing awareness and training initiatives on security for all personnel.

LIST OF ABBREVIATIONS

ABE	Attribute Based Encryption
AES	Advanced Encryption Standard
AVE	Average Variance Extracted
BYOD	Bring Your Own Device
DAC	Discretionary Access Control
DDoS	Distributed denial of service
E-Health	Electronic Health
EHRs	Electronic Health Records
EMR	Electronic Medical Record
GHSA	Global Health Security Agenda
GOARN	Global Outbreak Alert & Response Network
HIT	Healthcare IT
IBE	Identity Based Encryption
IBPRE	Identity Based Proxy Re-encryption
HIS	International Health Security
IP	Internet Protocol
IT	Information Technology
LMICs	Low- and middle-income countries
MAC	Mandatory Access Control
Medjack	Medical Device Hijack
MFA	Multifactor authentication
MTRH	Moi teaching and Referral Hospital
NHS	National Health Service viii
PHI	Protected Health Information
PKE	Public Key Encryption
PKI	Public Key Infrastructure

SEM Structural Equation Modelling

WHO World Health Organizations

TABLE OF CONTENTS

LIST OF EQUATIONS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Overview

This chapter is an introduction to emerging system survivability threats and vulnerabilities in health systems. The rapid growth in technology has led to exposure to many threats and vulnerabilities in the health sector thus the need to have systems developed with survivable qualities in developing systems for hospitals, this chapter addresses the background of the problem, statement of the problem, objectives, research questions, significance of the study, Justification of the study, the scope of the study, definition of terms and the chapter summary.

1.2 Background of the Study

Survivability refers to a system's capacity to maintain essential services amidst attacks and failures, as well as its ability to restore full services promptly. The concept of survivability is regarded as a fundamental characteristic of a dependable system. A resilient system maintains its operational integrity, even in the face of malicious incursions or unforeseen failures. Even when a system possesses clearly delineated functions and accurate implementations, this does not ensure its survivability. Certain damages, arising from innovative and meticulously coordinated malicious attacks, are fundamentally beyond the predictive capabilities of the majority of system developers. In such scenarios, even a resilient system with thoroughly defined security measures may still be vulnerable to compromise.

Globally Information technology serves as an exceptionally significant instrument within contemporary organizations. Contemporary organizations are propelled by the advent of emerging technologies, which, upon implementation, enhance client welfare and transform interpersonal interactions while fostering social engagement. (Denert, 2020). Across the African continent, numerous nations have experienced an increase in the documentation of digital threats and nefarious activities. The outcomes encompass compromised public infrastructure, financial losses stemming from digital fraud and illicit monetary transfers, as well as national security violations characterized by espionage and intelligence theft perpetrated by militant organizations. Although the various governments across the continent appear to be sluggish in recognizing the significance of information systems safety, the regional political entity, the African Union, seems to be making strides in enhancing awareness and promoting improved cyber safety, particularly among the continent's ministers of Information and Communications Technology. The COVID-19 pandemic that came in 2019 has illustrated the weaknesses within health systems among several African nations, remarkably in south of the saharan Africa. Prior to the Covid-19 in Africa, the challenges with the health background were fundamentally characterized by fragile health systems, inadequate governance and accountability, elevated levels of out-of-pocket expenses, detrimental social determinants of health, and a lack of direction in health support and provision of services. Throughout the pandemic, a notable transformation in the approach to fortifying health systems has taken place, focusing on enhanced financial investment

in health infrastructure. This initiative aims to address the following areas: the enhancement of health systems, the encouragement of the health personnel, and the advancement of laboratory amenities. The expectation is the implications of enhancing health approaches in Africa post-pandemic may be sustained through a continental peer-review mechanism designed to oversee adherence to augmented financial support for the health sector between affiliate nations. (Uwaezuoke, 2020)

Kenya is rapidly embracing innovation and is increasingly transforming into a nation reliant on electronic transactions. However, without a comprehensive national digital security strategy in place to identify the risks we face, it will be a challenging endeavor. Kenya stands as a prominent figure in the digital economic landscape of Africa. The nation has experienced a profound transformation in the digital realm since the early 2000s; consistent investment in connectivity infrastructure, alongside a resourceful citizenry, has resulted in the information, communications, and technology (ICT) sector expanding by an average of 10.8 percent annually since 2016.The Ministry of Information (2019) delineates aspirations to utilize ICT as a cornerstone for establishing a more resilient economy, aiming to enhance the sector's contribution to both the digital and traditional economy to 10 percent of gross domestic product by the year 2030. Embracing a continental leadership position, Kenya formulated a Digital Economy Blueprint in 2019, leveraging the nation’s digitalization experience to suggest a framework that other African nations might consider for investing in their respective digital economies. According to Cremer F (2022), there has been a significant increase in the number of system attacks targeting our public,

private, and predominantly financial institutions, resulting in losses of approximately 2 billion within that year. It is essential to recognize the perils facing the internet, particularly in relation to electronic transaction systems. One must examine the factors that contribute to these threats and ultimately develop a framework and strategy aimed at mitigating future attacks, while also exploring increasingly innovative methods to safeguard our sensitive information.Hospitals are increasingly reliant on technology to execute fundamental tasks, with a significant portion of operations being automated. This results in hospitals depending on information technology systems for their operations.

The integration of E-Health within hospitals and various medical establishments has been profound, with nearly all facets of medical care having undergone some form of computerization. This encompasses the digitization of medical records, diagnostic devices (such as ultrasound), point-of-care assessment instruments (like glucometers), patient monitoring systems, and software for the planning and management of healthcare professionals (SG., 2020). The shift towards digitization has raised significant concerns regarding accessibility, alongside potential threats to safety and privacy for patients, with Kenya emerging as a notable target for systemic crimes. The investigation into IT practices within medical environments has revealed persistent discrepancies between the theoretical frameworks of healthcare personnel and the implementation of IT infrastructure. The growing adoption of mobile technology by both patients and healthcare institutions has further compounded the challenges that hinder the mitigation of system survivability attacks. Healthcare technologies possess the capacity to broaden, preserve, and elevate the quality of human existence. The spectrum of technologies encompasses electronic health record storage systems, safety monitoring devices, and medication distribution technologies, which include both general-purpose devices and wearables, as well as innovations

integrated within the human body. Additionally, telemedicine technologies facilitate remote treatment, transcending geographical boundaries. Patients are progressively engaging with their personal smartphone applications, which can now be integrated with telemedicine and telehealth for the purpose of coordinated disease management and care planning within the framework of the Health Internet of Things (Haleem A, 2021).

As healthcare technologies continue to advance, their interconnectivity and interoperability with various systems also expand, leading to the emergence of E-Health systems. Many are now incorporated into the hospital network, whereas they were traditionally independent. Numerous advantages arise from interconnection, including enhanced efficiency, diminished errors, automation, and the capability for remote monitoring. The advantages significantly alter the management of both acute and persistent chronic conditions (Serrano LP, 2023). The integration of technology beyond clinical settings enables healthcare practitioners to oversee and modify implanted devices, eliminating the necessity for hospital visits or invasive interventions. The implementation of electronic health records has the potential to enhance patient care by facilitating broader access to health-related information. Regrettably, interconnection introduces additional vulnerabilities in the resilience of systems against attacks. The interconnectivity of contemporary records, however, presents numerous potential avenues for access; the capacity for remote access (in contrast to historical records in hospitals, which were secured and could only be accessed through physical means); the possibility of data theft occurring without detection; and the availability of a more extensive health record, which serves as a more significant resource for potential assaults. In the past, the loss of paper records or the theft of a laptop could have compromised the privacy of hundreds or thousands of

patients. However, with the transition to electronic records accessible across various networks, the risk of privacy invasion now extends to potentially millions (Seh AH, 2020). Moreover, the health records of celebrities have proven to be a significant focus for compromise.

Prior to the advent of electronic documents, such violations were confined to hospital personnel who had the ability to access the physical records (Ismail Keshta, 2021). With the advent of remote access to celebrity health records, the likelihood of breaches is poised to escalate. Nonetheless, electronic records present a significant privacy benefit compared to their paper counterparts: the capacity to monitor staff access. A recent report suggests that over fifty percent of violations in healthcare stem from within the organization (Tsai CH, Effects of Electronic Health Record Implementation and Barriers to Adoption and Use: Life, 2020). While it was once challenging to ascertain who had a preliminary view of paper medical records, the tracking of individuals accessing electronic records has become significantly more straightforward. While there are more advanced and external methods available for assailants to achieve this. This thesis presents a comprehensive framework aimed at facilitating the design of autonomous health systems, thereby augmenting their efficacy in intricate environments. Within this framework, survivability emerges as a critical operational requirement for an autonomous system, integrated into its system architecture and design considerations. This Survivability Framework is designed to integrate the comprehension of physiological, psychological, and cognitive mechanisms that underpin the capacity of biological systems to endure challenging environments, particularly in the face of threats.

1.3 Statement of the problem

The health care facilities and units, along with other sectors that closely coordinate or provide services to these establishments, predominantly depend on the exchange of information. For the sake of convenience in access, storage, and retrieval, information and communication technology (ICT) proves to be quite beneficial. The rapid advancement of this technology, coupled with its increased accessibility and reduced costs, has consequently resulted in both beneficial and detrimental transformations within the healthcare sector as a whole. The rise in connectivity and interoperability has been observed to lead to numerous additional instances of system insecurity, vulnerability, and challenges related to survivability. Ndlovu K (2021) asserts that the rise in accessibility, accompanied by substantial capacity, inevitably leads to heightened vulnerability. “Providing the advantages of digital healthcare.”

Despite significant progress in the development of secure systems, a limited number of health systems demonstrate the ability to function effectively in real or uncontrolled conditions, particularly when faced with unforeseen circumstances and environments that exceed their original design parameters (health systems are capable of operating in real or uncontrolled conditions, 2021). The successful implementation of these systems necessitates elevated reliability, quantifiable safety standards, and the capacity to endure unforeseen circumstances (Technology, 2023). Nonetheless, these capabilities remain difficult to attain, and significant technological hurdles persist that require attention. Given the multitude of attacks that prevail in contemporary society, it is imperative to devise systems capable of enduring and delivering services even amidst and following such assaults. Consequently, the nation continues to grapple with these pressing issues, particularly within critical domains such as the healthcare sector. This research aims to fill this void and establish a comprehensive framework.

1.4 Objectives

The main objective of this study was to determine the emerging threats, assess their effects in health Care and to develop a robust Framework that hospitals can implement to mitigate the system survivability threats.

1.4.1 Specific objectives

a) To identify the emerging threats and vulnerabilities in health facilities.

b) To determine the effects of the system survivability threats to the health facilities.

c) To determine system survivability Mitigation Factors

d) To develop a system survivability threat Framework For the threats facing health facilities.

1.5 Hypothesis

The null hypothesis developed from the conceptual framework of the study was as follows.

a) **H**– Top management commitment does not influence survivability and security of systems threats in health sector.

b) **H** – IT policies does not influence systems survivability threats in health sector.

c) **H** – Organizational factors does not influence the systems survivability threats in health sector.

d) **H –** IT Literacy does not influence systems survivability threats in health sector.

e) **H** - Existence of challenges/ threats does not mediate the relationship between organizational individual factors and systems survivability threats in health.

1.6 Research Questions

a) What are the emerging threats and vulnerabilities that affect the system survivability?

b) What are the effects of system survivability in health facility system?

c) What are the survivability Mitigation Factors?

d) How is survivability framework currently guiding systems survivability and security developments?

1.7 Justification of the study

Conventional methodologies for safeguarding information systems have primarily concentrated on thwarting the success of attacks by fortifying the system through an array of security measures. Numerous studies have indicated that security measures can safeguard one layer of a networked system; however, they frequently create vulnerabilities in other layers. Moreover, although security serves as a method to safeguard system modules, survivability represents a more elevated objective than security, as it encompasses the operational integrity of the entire information system rather than merely its individual components. In the event of accidents or assaults, certain elements of the system may experience failure; however, this does not inherently lead to catastrophic outcomes. The system has the potential to endure, provided that essential services are upheld. This ought to be approached through the lens of survivability rather than security. The concept of survivability has been examined from various perspectives, focusing on the essential capabilities that a critical system must possess.

The concept of system survivability encompasses a broad range of considerations that are increasingly significant in our interconnected world, where systems play a crucial role in facilitating essential transactions. While an ideal resolution to combating systemic crimes remains elusive, it is imperative that individuals endeavor to mitigate and manage these offenses to foster a safer environment in the future. This statement holds true; therefore, it is imperative to establish a framework applicable not only to security solutions but also to the survivability of systems. Any information system that delivers essential services to the nation and society must be both reliable and dependable. Given the fundamental importance of these systems to societal well-being and their frequent targeting by malicious entities, it is imperative that we ensure these systems possess the requisite resilience to withstand potential attacks, all while maintaining sufficient service levels to support the critical operations of our healthcare facilities.

The framework presented in this paper aims to examine survivability from a unique vantage point. The text delineates the methodologies and mechanisms employed for reasoning and articulating the requirements for system survivability as determined by a user. Considering the extensive scope and diverse nature of health systems, it is essential for the user to ascertain their specific requirements regarding the survivability features of the systems intended to uphold mission-critical functions.

1.7 Significance of the study

This work intended to elucidate the nature and features of threats present inside the health division in Kenya. The objective is to evaluate the emerging threats and vulnerabilities that impact the

health sector in Kenya, with a particular focus on Moi Teaching and Referral Hospital. The research aimed to establish and validate a framework intended for adoption by the hospital and the broader health sector in Kenya. The framework established by the study focused on the human, organizational, and policy dimensions of the threats. This endeavor is aimed at addressing systemic threats within the healthcare sector. This study makes a significant contribution to academic discourse. Investigations centered on the identical subject matter in Kenya remain insufficiently explored, notwithstanding the continuous expansion and reliance on ICT systems, alongside certain occurrences of insecurity. The study enriches understanding within the domain of information system survivability and highlights areas where knowledge is lacking, paving the way for future research endeavors.

The research provides a deeper understanding of critical matters related to system survivability in healthcare facilities, equipping security managers and other key stakeholders with the knowledge necessary to effectively address these threats within their organizations and optimize the use of available system resources to fulfill their objectives. The research further empowers public sector policy makers to critically reassess and refine current security strategies, aiming to establish a robust IT-based security infrastructure for future applications. It provides additional insights that enhance the foundational comprehension in the field of data protection and encourages further inquiry in this significant area of Research.

1.8 Scope of the study

The health sector is extensive and encompasses Community Services, Dispensaries, Clinics, Health centers, maternity and nursing homes, Sub-County hospitals, medium-sized private

hospitals, County referral hospitals, large private hospitals, National referral hospitals, and large private teaching hospitals. Given the substantial volume of clients, the implementation of health systems has become essential. Given the extensive nature of the health sector, this study focused specifically on (MTRH), recognized as the next greatest national hospital after (KNH). Data was gathered from the IT staff and various departmental employees to identify the emerging threats and vulnerabilities within the hospital, employing a descriptive research design. The Hospital caters to the inhabitants of 24 counties in Kenya, as well as regions of Eastern Uganda, South Sudan, Tanzania, and the Democratic Republic of Congo, encompassing a population exceeding 25 million individuals. The hospital possesses a capacity of 1,020 specialized beds, accommodating an average of 1,300 inpatients at any given moment, alongside serving approximately 1,500 outpatients daily. The array of specialized services encompasses Oncology services, including Radiotherapy, Brachytherapy, and Chemotherapy; Intensive Care Unit (ICU) Services; Kidney transplants; rehabilitative services for Alcohol and Drug Abuse; Spine and Neurosurgical operations; Cardiology and Cardiothoracic services; open heart surgery; corneal transplants; and Arthroscopic surgeries for the Shoulder and Knee, as well as Phototherapy and Wound care. Additional methods include Postpartum Intrauterine Devices (PPIUD) and surgeries conducted within a 24-hour training framework. These specialized services align with the principles of Universal Health Coverage (UHC) and Kenya's commitment to enhancing and expanding access to advanced healthcare for all individuals. Throughout the years, the Hospital has undergone significant expansion across various domains, including infrastructure development, the volume of patients served, the complexity of diagnoses, and the increase in Human Resources for Health (HRH). This progress positions it as the Next big health facility in the country, as per the Kenya Harmonized Health Facility Assessment (MOH, Kenya Harmonized Health Facility Assessment,

2018/2019). The deployment of the Health Management Information System at MTRH includes a variety of system components such as Medical Records, Outpatient Module, Inpatient Module, Pharmacy Module, Laboratory Module, Radiology Module, Consulting Doctor, Fiscal Management, and Supply Chain Management.

1.9 Definition of terms

Breach – When an individual adept in the art of hacking skillfully exploits a vulnerability within a computer or device, thereby obtaining unauthorized access to its files and network. (Lakshmanan, 2020)

Computer hardware vandalism - refers to the deliberate act of dismantling or damaging computer hardware. A student might intentionally inflict harm on a laptop provided by a school.

Cybercrime – As articulated by Lakshmanan (2020), cybercrime encompasses criminal activities executed through the utilization of digital devices, such as computers, via the internet.

Cybervandalism - refers to harm or obliteration occurring in a digital context. Cyber vandals engage in activities such as defacing websites (for instance, Wikipedia), developing malware that compromises electronic files or disrupts normal functionality, or physically removing a disk drive to incapacitate a computer system, as noted by (Complete Network, n.d.).

Ransomware – A type of malicious software that intentionally obstructs your access to files on your computer, effectively taking your data captive (https://en.wikipedia.org, 2024). Files are usually encrypted by ransomware, which demands payment to have the files unlocked or restored.

Survivability - Survivability denotes a system's ability to maintain critical services amidst adversities and disruptions, as well as to restore complete functionality promptly when conditions become favorable, as articulated by Nasibeh Zohrabi in 2019. In the realm of critical systems employed in national defense, healthcare, and utility infrastructure, the imperative of survivability stands as a fundamental requirement.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

Hospitals and clinics all over the world are becoming increasingly connected posing a major risk to the health sector. The review of literature is covered in the following order: A review of trends and threats in the health sector and how the sector can move further from the attack to deliver to have the same system delivering its mandate, Many different security interventions being used in e-Health, advantages and disadvantages of each of the approaches has been identified and a review of ransomware as one of the most common attacks on the health sector. The study also reviewed various theories that are believed to guide this study.

2.2 Emerging Survivability Threats and Vulnerabilities in the Health Facilities

2.2.1 System survivability Concerns in Healthcare

It was widely believed that healthcare programs would be safe from attack, hence no security precautions were thought necessary. No healthcare agency exists to ensure the security of the system. The emphasis has historically and justifiably been placed on patient care. Numerous factors contribute to the complexities surrounding the survivability of health care systems, which have heightened their vulnerability over time (Kruk ME, 2018).

Advancing interconnected technology to facilitate effective approaches to patient care, particularly in the management of chronic conditions. This provides various methods for establishing connections with medical devices. The frequent accessibility of devices significantly heightens the

probability of their discovery by potential attackers (Samal L, 2021). A solitary device may serve as a possible gateway for expansive hospital networks, circumventing the security measures established by firewalls. Additionally, there exists a propensity for a temporal delay occurs between the happening of an attack and the follow-up detection of a breach, or even the recovery process, which can hinder the system's ability to perform its essential functions, thereby exacerbating vulnerability. Increased emphasis on maintaining patient health results in enhanced continuous monitoring of individuals beyond the confines of clinical environments. The proliferation of devices within the expansive healthcare landscape heightens the susceptibility to breaches. The extensive proliferation of mobile consumer devices, particularly smartphones, complicates the safeguarding of health data against the inherent risks associated with commonly used devices (avad Pool, 2024).

Alongside the surge in emerging technologies, numerous healthcare organizations continue to rely on outdated systems, such as Windows XP, which has not received support since 2014 (Milliman, 2016). This reliance facilitates the evasion of detection by hackers and malware, as evidenced by the recent WannaCry attack. The inherent constraints of medical device software imply that healthcare IT teams often lack access to the internal workings of these devices, necessitating a dependence on manufacturers to establish and uphold security measures that may be insufficient. Additionally, there exists a significant issue regarding insufficient funding allocated for system survivability. While hospitals and various organizations invest resources to enhance integration, they fail to dedicate adequate time and financial support towards maintaining updated software and ensuring system security (Tsai CH, Effects of Electronic Health Record Implementation and Barriers to Adoption and Use:, 2020). This situation is further intensified by an absence of specialized knowledge in system survivability security, stemming from a widespread deficiency in

technological resources and the significant costs associated with security personnel. In conclusion, the swift changeover to electronic health records and interrelated devices, coupled with a historical and persistent underinvestment in system survivability and a limited comprehension of the safety work behaviors of health personnel, has rendered the health sector susceptible to attacks.

While the healthcare sector presents certain vulnerabilities, it is essential to recognize that attackers must possess a compelling motivation to engage in such malicious activities. Motivation encompasses the prospects of financial and political advantage, as well as the potential for loss of life within the context of cyber warfare. The foremost of those motivations is the economic advantage. The significance of health care data surpasses that of any other type of data. The worth may surpass €888.05 for an entire collection of medical credentials (https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/, 2024). Illegally obtained medical identification can be exploited to assume another individual's identity or insurance information, thereby facilitating access to healthcare services and prescription medications. Applications encompass the realm of organized crime, executing intricate schemes of deception. In recent years, individuals engaged in deceitful practices have amassed billions by submitting false claims and distributing pharmaceuticals for sale on the dark web (Crime, 2022). At times, medical records contain ample information that can facilitate the opening of bank accounts, the securing of loans, or the acquisition of passports.

2.2.2 Effects of Cybercrime on Healthcare

Since 2015, hacking has emerged as the predominant factor contributing to breaches of health sector inmformation(Lakshmanan, 2020). Malware, including ransomware, presents significant

challenges. Cybercriminals persist in taking advantage of inadequate security measures to unlawfully access health documents, challenge access to medical services, or Impose intentional damage. The healthcare industry has experienced a significant Increase in both the volume and magnitude of data security Crimes over recent years. Incidents resulted in financial detriment, damage to our data integrity, and poor patient safety.

In Australia, it has been reported that the medical card numbers of every citizen are accessible for purchase on the dark web (Javad Pool, 2024). The Ponemon Institute has recently disclosed that the average expense associated with the loss or theft of medical records, which encompass confidential and sensitive information, amounts to €337.46. The ongoing promotion linked to significant breaches could undermine patient trust, potentially leading to a decreased willingness to share data (Javad Pool, 2024). This presents a significant challenge for individuals suffering from conditions that are often subject to stigma, including those related to sexual and mental health.

In light of the numerous warnings disseminated and the presence of security patches—many of which remained uninstalled—the magnitude of the WannaCry attack in 2017 was indeed remarkable. The WannaCry ransomware has infiltrated over 300,000 computers globally, coercing users into paying ransoms in bitcoin (Office, 2018). A total of fifty hospitals across the UK have encountered comprehensive system lockouts, resulting in delays in patient care and impairments in the functionality of interconnected devices, including MRI scanners and blood storage refrigerators. This assault was not aimed exclusively at healthcare institutions; however, the repercussions were extensive. Additional ransomware has been directed explicitly at the healthcare sector. Mansfield-De-vine indicates that a variant of ransomware affected approximately fifty percent of NHS trusts in the UK during the period from 2015 to 2016. (Spence, 2018). The case of

the Hollywood Presbyterian Medical Centre, which was incapacitated for 10 days until it acquiesced to a ransom of €15096.88, received significant attention from US media; this incident is believed to have stemmed from a phishing email (Raburu, 2021).

A multitude of malware attacks has precipitated significant incidents, exemplified by a particular UK healthcare trust that endured an unspecified cyber-attack, culminating in the cessation of its IT systems and the cancellation of nearly all scheduled operations and outpatient appointments for a duration of four days (Raburu, 2021). Another incident referred to as Medjack ("Medical Device Hijack") involves the insertion of malware into unprotected medical softwares, facilitating lateral movement within the hospital network (Raburu, 2021). Contaminated medical devices undermined the integrity of hospital safety protocols, encompassing diagnostic apparatus such as MRI machines, therapeutic devices like distillation pumps, and essential life-sustenance equipment, including ventilators. This apparatus had not been previously recognized as a platform for wider assaults. Illness may subsequently propagate to additional devices, such as a nurse's workstation, which possesses access to medical records and internet connectivity to transmit data to the attackers.

Simulated attacks conducted by ethical hackers have underscored the existence of additional vulnerabilities, indicating that medical devices may represent the forthcoming security crisis. There exists a possibility for assaults reminiscent of what was once relegated to the realm of speculative fiction. For instance, the concept of brain jacking involves the insertion of a suitable device (Raburu, 2021). Simulated assaults on devices including pacemakers, defibrillators, insulin pumps, and drug infusion pumps have been executed. These assaults involve the manipulation of machines from a distance to alter surgical procedures or administer fatal quantities of medication. While these attacks are presently only simulated, their occurrence may be anticipated (He Y & do,

2021). The potential for risks will persistently escalate if cybersecurity measures are not integrated from the inception of the product or project lifecycle.

2.2.3 Ransomware and other Malware

Malware presents a significant trial through various sectors; nevertheless, in the realm of healthcare, a malware infection can have dire consequences, potentially determining life or death outcomes. Healthcare functions through a complex network of interrelated reporting and services. The intricate system that conveys evidence on our behalf to enhance our well-being is particularly susceptible to ransomware and various forms of malware attacks. During the previously discussed NHS WannaCry incident, health centres were compelled to halt admissions for new patients, while ongoing treatments for existing patients were disrupted due to the inaccessibility of medical records. The HHS 'Wall of Shame' specifies healthcare records attacks in the United States, currently documenting 288 incidents that have impacted nearly 4.7 million individuals from the start of the year up to January 1, 2018. As reported by Proofpoint, in the first quarter of 2017, the number of ransomware variants detected was fourfold greater than that of the preceding year. The healthcare sector ranks prominently among industries that are frequently targeted by cyber criminals (Raburu, 2021). Incidents may arise from unauthorized access, malicious software, and risks posed by internal actors. Insider threats arise from both inadvertent mistakes and intentional misconduct by employees, such as engaging with phishing emails, falling victim to social engineering strategies intended at gaining login authorisations or introducing malware attacks, misconfiguring security settings, mismanaging passwords, misplacing laptops, and transmitting unencrypted emails. This consequently emerges as a moderating factor alongside DDOS and ransomware attacks.

Ransomware capitalizes on weaknesses to seize financial systems for the purpose of extracting sensitive information within the realm of information technology (IT). The intrinsic nature and significance of information render access to medical data a conduit for cyber criminals to perpetrate identity theft, engage in medical fraud, extort individuals, and unlawfully acquire controlled substances. The utility and versatility of medical information, along with the extensive centralized storage of such data, the relatively weak IT security systems, and the expanding use of healthcare IT infrastructure, all serve to heighten the risk of cyber-attacks on healthcare institutions. Studies indicate that a person's medical data holds a value to cyber-criminals that is 20 to 50 times greater than that of personal financial information (Raburu, 2021). Consequently, there is a notable annual increase of 22% in cyber-attacks aimed at medical information (Raburu, 2021). Ransomware employs a sophisticated hybrid encryption system that integrates two forms of cryptography to establish an asymmetric cryptosystem. In this framework, data is first encrypted with a randomly generated symmetric key, which is subsequently secured using a public key, accessible only to the party possessing the corresponding private key (Halsey, 2022). The cyber-criminal employs the private key to decrypt the symmetric key, subsequently transforming the data back into "plaintext" and returning the key to the victim, who can then regain access to their device (Halsey, 2022). When subjected to encryption, the code becomes inaccessible and incomprehensible. A pop-up notification is presented to the user, demanding a ransom payment, typically in an untraceable digital currency like bitcoin, in return for the decryption key (P. Stawicki, 2021).

Ransomware frequently does not obliterate data; rather, it encrypts it, rendering it inaccessible until a ransom is remitted. Even after the eradication of the ransomware infection, the data may still remain in an encrypted state. However, it is essential to acknowledge that the mere presence of

ransomware on a computer does not constitute a complete understanding of the situation. In order to obtain an encryption key and subsequently report its findings, the ransomware is required to establish communication with a server (Spence, 2018). This encompasses a server operated by a corporation that eschews illicit activities and guarantees anonymity for the perpetrators, commonly referred to as Bulletproof Hosting. Such enterprises are frequently situated in China or Russia (Spence, 2018).

In the event of a ransomware attack, malicious software is introduced into a network, leading to the infection and encryption of sensitive data until a specified ransom is remitted. Following an assessment done last year, ransomware attacks denote an progressively considerable menace to healthcare systems. In the year 2020, around one-tertiary of healthcare associations global faced the consequences of a ransomware attack.
The reason for its widespread occurrence lies in the comprehension that hackers possess regarding the imperative nature of minimizing operational disruptions within the healthcare sector. In the episode of a ransomware attack, health providers often find themselves in a state of distress, apprehensive about the regulatory repercussions that may ensue from the compromise of patient data.

2.2.4 Phishing

Similar to other sectors, the healthcare industry faces vulnerabilities to phishing threats. A study by Verizon reveals that about 66% of malware stood commenced through electronic message

attachments (Morrow, 2018). While it is improbable that the WannaCry ransomware originated from an email, a significant amount of malware persists in being deployed through phishing methods. Nonetheless, phishing emails and texts pose a significant risk to individual information, encompassing login identifications.

The (NHISC) has lately indicated that the healthcare sphere stands currently facing the highest vulnerability to predative emails. Nevertheless, minimal action has been undertaken to address this issue, as evidenced by the fact that 98% of healthcare organizations have yet to initiate preventive measures against phishing by implementing Domain-based Message Authentication, Reporting & Conformance (DMARC) (Morrow, 2018).

2.2.5 Insider threats

Insider hazards to clinic assets present a significant trouble universally, potentially originating from both patients and staff, and manifesting in forms that are either intentional or inadvertent. The 2017 HIMSS Cybersecurity Survey revealed that 75% of respondents considered insider threats sufficiently concerning to warrant the establishment of dedicated protective programs.

2.2.6 Spoofing

Spoofing refers to the act of concealing one's true identity to avoid being discovered for illicit activities, while simultaneously impersonating another individual to establish trust and acquire sensitive information from systems. The prevalent practice of altering the hardware or MAC address is referred to as MAC cloning, while the modification of the IP address or unique identity

within a network is known as IP spoofing. Additionally, the act of masquerading as another individual in digital correspondence is termed email spoofing. (Morrow, 2018)

2.2.7 Information-gathering attacks

The process of information gathering involves an assailant acquiring invaluable insights regarding potential targets. This should not be construed as an assault; rather, it represents a preliminary stage of potential aggression, characterized by its entirely passive nature, as there is no overt act of hostility present. Systems such as computers, servers, and network infrastructure, encompassing communication links and inter-networking devices, undergo processes of sniffing, scanning, and probing to collect data around the operational position of the objective system, the availability of open ports, and specifics concerning the operating system and its version, among other details. Among the various techniques employed for information gathering are sniffing, mapping, vulnerability scanning, and phishing, among others.

2.2.8 Password attacks

One of the most straightforward methods to gain control over a system or any user account is by employing a password attack. When the personal and behavioral characteristics of the victim are understood, the assailant begins by attempting to deduce the password. Often, the assailant employs various techniques of social engineering to uncover and ascertain the password. A dictionary attack represents an advanced phase in the realm of password breaches and operates through automation.

2.2.9 Virus

Computer viruses represent a significant collective threat to users of computer systems. Computer viruses represent a form of malicious software engineered to propagate from one computer to another via file transfers, often attaching themselves to legitimate programs and operating systems, or through email communications. Email attachments or downloads from websites can compromise the integrity of the computer and potentially affect other devices within its network of contacts through the communication infrastructure. Viruses exert a significant impact on system security by altering configurations, accessing sensitive information, presenting unsolicited advertisements, disseminating spam to contacts, and commandeering the web browser, as noted by Thomas C. in 2020. The viruses can be classified into executable viruses, boot sector viruses, or e-mail viruses.

2.2.10 Worms

Computer worms are segments of harmful software that replicate rapidly and propagate from one computer to another via its connections, subsequently disseminating to the contacts of these additional systems, thereby extending their reach to numerous devices in a remarkably short period. Intriguingly, worms are meticulously engineered for dissemination by leveraging software vulnerabilities. Worms exhibit unsolicited promotional content. This process consumes significant CPU resources and network bandwidth, consequently obstructing access to the victim's systems or network, resulting in disorder and eroding trust within the communication network.

2.2.11 Trojans

Trojans are software applications that present themselves as entirely legitimate while concealing a harmful component within their structure. Trojans are typically disseminated via email attachments from seemingly reliable contacts and by engaging with deceptive advertisements. The payload of Trojans consists of an executable file designed to install a server program on the victim’s system by opening a port that remains perpetually active, while the server operates from the attacker’s system. Consequently, whenever the assailant seeks to access the victim's machine, they can accomplish this through the concealed backdoor entry, rendering it imperceptible to the user.

2.2.12 Spyware and adware

Spyware and adware are types of software characterized by their tendency to gather personal information from users surreptitiously. Adware is designed to monitor the user's browsing habits, subsequently generating pop-ups and advertisements tailored to that data. Spyware, conversely, is surreptitiously installed on a computer, collecting data regarding the user's online behaviors without their awareness. Spyware incorporates keyloggers that meticulously document every keystroke, rendering it perilous due to the significant risk of identity theft.

2.2.13 Botnets

A compilation of compromised systems or bots functions as a collective of infected computers, governed by a bot master, to execute remote control and orchestrate synchronized assaults on a targeted host. This assemblage of bots, agents, and their orchestrators forms a cohesive botnet. Botnets serve the purpose of disseminating spam and executing distributed denial of service attacks.

2.2.14 Denial-of-service attacks

Denial-of-service (DoS) attacks, as the term implies, obstruct users from gaining access to or utilizing the service or system. This primarily occurs through the saturation of bandwidth, CPU, or memory, resulting in the denial of access to the network of the targeted machine or server providing the service. Denial of Service attacks consequently disrupt the functionality of computer or network systems, rendering them either inaccessible or significantly diminished in performance.4.16 Distributed DoSIIn distributed DoS (DDoS) attacks, the target is assailed by numerous individual compromised systems concurrently. DDoS attacks are typically executed through the utilization of botnets. The botmaster serves as the orchestrator of an indirect assault on the victim machine, employing a legion of bots or zombies to execute the attack. DDoS attacks manifest when numerous compromised systems operate in unison, orchestrated by an attacker to deplete resources entirely, thereby compelling the target to deny service to legitimate users. The increase in traffic volume burdens the website or server, resulting in a sluggish appearance. Thomas C. Enhancing the performance of intrusion detection systems through advancements in sensor fusion (Morrow, 2018).

2.3 Factors Influencing system survivability attacks in healthcare.

It is imperative that the top management conveys to their employees the significance of systems survivability, facilitates efficient participation, and encourages individuals to take ownership and manage their responsibilities (Raburu, 2021). It is imperative that they allocate resources towards a solution that serves the collective interest and subsequently assess its efficacy. Moreover, organizational resources are often insufficient, as many organizations lack the necessary industry expertise to address survivability attacks, which is compounded by a general deficiency in technology and the high costs associated with security personnel.

Game theory examines the inherently self-serving and confrontational behaviors of both the attacker and the system administrator, while also evaluating the possible strategies that incorporate the human dimension of cyber security (Anwar, 2020). Securitization theory posits that there exists a prevailing perception of insufficient awareness and information regarding systems security issues in Kenya, which contributes to IT literacy being viewed as an individual factor. In the realm of systems survivability, the concept of intersectionality enhances our comprehension of system attack issues, revealing that they transcend mere technicalities to encompass legal, governmental, cultural, and economic dimensions. This multifaceted understanding ultimately informs the formulation of IT policies aimed at bolstering cybersecurity.

Drawing from the aforementioned literature review, the researcher sought to examine both organizational and individual factors, along with mediating elements, to develop a comprehensive framework for system survivability. The researcher sought to formulate and substantiate a

framework that encompasses the human factors, organizational culture, and IT policies related to system survivability within the health sector.

2.3.1 Increased use of Cloud computing and online security

Healthcare is increasingly adopting cloud computing due to its advantages, including enhanced data accessibility and cost-effectiveness. The adoption of Cloud computing in the healthcare sector is projected to experience a remarkable compound annual growth rate of 20.5% by the year 2020. However, cloud computing introduces its own set of risks. (Kravchenko, 2021)
It is imperative that data housed within Cloud repositories is adequately safeguarded, in alignment with recommendations from organizations such as OWASP. Safeguarding data both in storage and while being transmitted among web services necessitates not merely strong encoding protocols but also suitable and efficient authentication methods, including second-factor certification and hazard-based approaches.

2.3.2 Internet-enabled healthcare attacks (Internet of Things, IoT devices)

Health systems has embraced Net-connected strategies in an effort to leverage health information for the enhancement of patient outcomes. Applications such as OpenAPS, which represent an heightened data-driven insulin delivery system, alongside Internet-enabled action followers that help in cancer management, remain leading the charge for the Internet of Things to enhance healthcare. Nonetheless, the Internet of Things is beset by well-documented security and privacy concerns. A multitude of healthcare-oriented IoT devices collect personal data, subsequently

stored in a Cloud repository for the purpose of analyzing various conditions, treatments, and related factors. (Jagadeeswari V, 2018) Security concerns, exemplified by DDoS attacks such as the significant Mirai Bot incident of October 2016, which exploit IoT devices, present a potential risk that could impede treatment. Another aspect is the safeguarding of personal data to avert exposure. The matter of redundancy presents significant concerns, particularly as an increasing number of hospitals rely on the internet to enable their systems. (Metty Paul, 2023)

2.3.3 Lack of Data Encryption

Safeguarding sensitive business data during transmission and while stored remains a practice that many industries have yet to adopt, even though its efficacy is well-established. The health care sector manages highly sensitive information and recognizes the serious implications of data loss – hence, HIPAA compliance mandates that all computers must be encrypted (Thakur (2019).

2.4 Theoretical foundation

Some of the threats and survival crimes involve misconduct that is either carried out through PCs or is at least connected to them. The availability of limitless information across the globe is indeed remarkable; however, it brings with it a considerable array of challenges. This research was informed by game theory, the theory of securitization, and the theory of intersectionality.

2.4.1 Theory of Securitization

Securitization theory represents a contemporary framework for inquiry that seeks to explore security issues with greater flexibility than traditional security studies. It is grounded in a fundamental comprehension of security's essence, as securitization studies endeavor to achieve a

more precise understanding of the actors involved in securitization, the specific problems or threats identified, the referential objects at stake, the motivations behind these actions, the conclusions drawn, and the contextual factors influencing these processes (Otukoya, 2024).

The securitization theory articulates a referent object as either the state or an entity, yet it may also be conceptualized as a systemic structure, exemplified by “the existence of states” (Otukoya, 2024). This theory employs multiple levels to elucidate the rationale behind specific occurrences, which are not rigidly delineated. The examination of these threats is approached from international, regional, and national viewpoints across different societal strata, alongside an analysis of how systemic insecurity proliferates through these levels and creates interconnections among them. Presently, there exists a prevailing notion that there is insufficient awareness and information regarding systems survivability risk issues in Kenya. The theory of securitization holds significance in this analysis, as the threat is systemic and necessitates prompt intervention from both private entities and governmental bodies. The research additionally utilized securitization theory to comprehend the nuances of insecurity and internet technology.

2.4.2 Game Theory

A multitude of researchers have devised security mechanisms through the lens of game theory, exploring various methodologies. These include employing a stochastic game to simulate network security scenarios (Xiaotong Xu, 2020), modeling DDoS attacks (BHUPENDER KUMAR, 2019), establishing physical and MAC protection layers (Larkin, 2019), and developing intrusion detection systems (Benaddi, 2022). In order to attain a system solution that is entirely dependable, it is imperative that the decision made by a single component takes into account the policies

governing all other components within the network, a task that encompasses a remarkably extensive domain.

When modeling and analyzing extensive search spaces that encompass a multitude of what-if scenarios, game theory proves to be quite useful. The theoretical framework examines the inherently self-serving and combative behaviors of both the attacker and the system administrator, while also evaluating the possible strategic approaches available to them. Furthermore, game theory possesses the capacity to evaluate a multitude of alternative scenarios prior to executing the appropriate course of action; consequently, it can significantly enhance the decision-making process of the network administrator (Picardo, 2023). The attacker typically concentrates on inflicting the greatest possible corruption within the system, whereas the defender seeks to mitigate the damage or maintain service continuity in the face of the assault. The objectives of the assailant intersect with those of the defender, thereby reinforcing the relevance of employing a game-theoretical framework to investigate matters of survivability in the face of attacks and concerns regarding privacy.

2.4.3 Theory of Intersectionality

(Board, 2022) addresses the challenge of ‘single-axis’ analysis, which compartmentalizes social inequality issues into distinct problems encountered by various classes, including ethnicity, gender, sexual orientation, or socioeconomic status. Such analyses frequently culminate in conclusions that disregard the larger context, fostering competitive tensions among various issues and disparities that permit the neglect of essential matters and pivotal concerns. Systems resilience Threats and social justice are distinct domains; however, the principle of

intersectionality is applicable to both. It is essential to transcend the binary debate of whether a primary issue pertains to Problem A or Problem B, and instead, focus on the interconnections among Problem A, Problem B, Problem C, and other associated matters. In addressing these threats, an intersectional approach allows for a deeper comprehension of how these issues transcend mere technicality, encompassing legal, governmental, cultural, and economic dimensions, among others (Taylor, 2019).

2.5 Review of Existing system survivability Frameworks in Health Sector

The evolution of information and communication technology has fundamentally transformed the prevailing methodologies in health-care practices worldwide. This phenomenon is notably evident in the gradual shift towards electronic formats of medical prescriptions, particularly in many of the world's most developed nations (Shao M, 2022). The requirement to unite and consolidate various electronic health information from diverse sectors, including health study laboratories, hospitals, and medical cover firms, has given rise to the perception known as electronic health (e-Health). It is observed that the various domains engaged in the distribution of medical information have complicated the management of the application, thereby highlighting the necessity for a elctronic-based setting that facilitates collective data sharing across numerous organizational spheres (Nureni Ayofe Azeez C. V., 2019). Cloud computing offers numerous advantages, particularly in facilitating the efficient transmission and prompt sharing of medical information. It also alleviated healthcare providers from the complexities associated with infrastructure management and afforded them numerous opportunities to engage with IT service providers. Numerous academic papers have identified that cloud computing provides a multitude of benefits, including scalability,

cost-effectiveness, and enhanced agility in the collective use of resources (Nureni Ayofe Azeez C. V., 2019).

Given the established understanding that conventional public key infrastructure presents significant challenges in terms of complexity and implementation time for cryptographic mechanisms, (Nureni Ayofe Azeez C. V., 2019) has delineated various pertinent cryptographic techniques aimed at enhancing the survivability and privacy of Electronic Health Systems. The performance analysis of these techniques was meticulously evaluated, encompassing Identity Based Encryption as well as novel Identity Based Proxy Re-encryption schemes. The evaluation revealed that the newly developed IBPRE demonstrates superior efficiency in re-encryption, thereby enhancing the protection of cloud health information. The limitation of this technique lies in the authors' inability to assess the performance of alternative encryption methods, thereby rendering their conclusions about the efficacy of the new IBPRE somewhat presumptive. Nureni Ayofe Azeez C. V. (2019) devised a specialized privacy and protected access control system exclusively for e-Health applications. Their design was accomplished through the integration of three distinct security models: Discretionary Access Control, Mandatory Access Control, and Role-Based Access Control. This synthesis resulted in a novel architecture that empowers healthcare providers and patients to define and establish access privileges, thereby enhancing system resilience. The primary constraint of this system lies in its capacity to function solely as an independent security framework for meeting the standards associated with electronic health records.

Sivan and Zukarnain (2021) demonstrated the application of a lightweight framework to articulate a Secure Health architecture, leveraging Transport Layer Security/Secure Sockets Layer to

safeguard server-based data exchange without necessitating an additional security layer. Secure Health encompasses a multitude of security features, including authorization, to ensure the protection of data both in transit and at rest. It offers a significant benefit by safeguarding against unauthorized access by outside objects to the system housing medical information. In additive to this, it assists the executive to discern inaccuracies within the provided information. Although this framework offers certain advantages, its primary limitation lies in its dependence on specific platforms, rendering it non-scalable. In a cloud-based environment, the security policy and framework should accommodate scalability and potential future expansion.

(Lin HY, 2023) suggested a safe patient-centered electronic health information system that uses the Proxy Re-encryption protocol to grant dependable access permission in a cloud-based setting. The framework comprising five primary phases employs Attribute-Based Encryption to facilitate patient-centered management of access rights. The examination of performance indicates both commendable and outstanding results for the scheme. The limitation lies in the inflexibility of alternative forms of distributed systems. Furthermore, the scheme lacks the capacity for scalability and flexibility. Throughout the evaluation, a restricted cohort of users was taken into account. A different secured model was introduced by (Nureni Ayofe Azeez C. V., 2019). The established framework relies on the Advanced Encryption Standard algorithm, which has been meticulously developed to safeguard patient information in accordance with the security policy. The security framework enables individuals to maintain information within a cloud-based ecosystem with both reliability and security as paramount considerations. The framework, comprising three distinct modules, guarantees a heightened standard of privacy and security. The limitation of this framework lies in its inability to accommodate all varieties of operating systems. The outcome is

contingent upon the operating system in use. The application of this concept in a practical context is indeed quite intricate.

(Alabdulatif, Thilakarathne, & Kalinaki, 2023) created a unique access-control mechanism in Electronic Health Record to address security and privacy issues. The framework embraced hybrid clouds alongside the evolution of access control policies to guarantee dependable and consistent access control, as well as permission-preserving data sharing among diverse healthcare providers. Certain cryptographic components were implemented alongside access control policy transformation to address the diverse access privileges and permissions of various EHR users across different cloud environments, thereby enhancing the model's efficiency. The primary limitation of this framework lies in its failure to provide users with the opportunity for expansion. It restricts scalability due to the finite number of users permitted.

To guarantee that e-Health care service providers minimize the expenses associated with data processing and online accessibility, Sivan and Zukarnain (2021) proposed a system for protection featuring multiple hierarchy levels. Providing centralized access control. The implementation of Attribute Based Encryption was executed in a manner that the ABE access structures delineated privileges and contrasted them into discrete roles. The primary challenge associated with this methodology lies in addressing the intricacies of analogous inquiries from diverse users, given that health information is managed through a centralized server. It is essential to establish priorities when multiple users make simultaneous requests.

Table 1: Summary of reviewed frameworks

Author	Year	Approach	Strength	Weakness
Wang *et al*.	2017	Identity Based Encryption (IBE) & new Identity Based Proxy Re-encryption (IBPRE) schemes	Newly developed IBPRE is better and efficient for re-encryption.	Performance of the model is not efficient and reliable
Gajana yake *et al*.	2012	Discretionary Access Control (DAC), Mandatory Access Control (MAC) & Role Based Access Control (RBAC)	Patients responsible for dictating and setting access privileges	It cannot be used in a distributed environment.
Simplic io *et al*.	2014	Transport Layer Security/Secure Socket Layer (TLS/SSL)	Prevents from unauthorized access	Platform dependent thus not scalable
Barua *et al*.	2011	Proxy Re-encryption	The schema has an excellent performance	No room for scalability
Sunaga r & Biradar	2014	Advanced Encryption Standard (AES)	Reliable in cloud-based environment	Operating system dependent
Rezaeib agha & Mu	2016	Hybrid clouds, access control policy transformation & cryptographic building blocks	Different access privileges for different EHR users.	No room for scalability
Barua	2011	Attribute Based Encryption	Privileges were mapped	Storage of

et al.	(ABE)	into various roles with ABE access structures	health information in a centralized server

To achieve optimal productivity and security in any e-Health application, it is imperative to implement a robust security framework capable of effectively addressing a range of threats, including bribery, denial of service attacks, identity spoofing, and any instances of unlawful or unauthorized privilege escalation. The security frameworks must also be capable of addressing the privacy and safety requirements that may arise due to the architecture of cloud systems. Public Key Encryption is extensively employed to meet various security needs, including those pertaining to anonymity, collusion, and unlikability (Dougherty, 2023). Nonetheless, given the broad and pervasive implementation of PKE infrastructure, it is imperative that the capabilities and efficiencies of PKE be refined and improved. Ensuring the integrity, confidentiality, reliability, and authenticity of health data in private, public, or hybrid cloud environments is of paramount importance.

Another significant safety initiative that has been deliberated is ABE. This security model fulfills certain criteria pertaining to protection and privacy. ABE has demonstrated exceptional fine-grained and patient-centric access to electronic data (Wang, 2020). Nevertheless, this approach renders the ABE-enabled scheme expensive when one takes into account the computational complexity involved. Moreover, a significant obstacle lies in the administration of access policies.

Given the extensive body of literature, particularly the ones examined above, it becomes evident that nearly all the current frameworks encounter various challenges. Numerous prevailing frameworks encounter obstacles including scalability, interoperability, flexibility, consistency, inadequate model assessment, challenges in integration within distributed environments like cloud computing, key management issues, as well as concerns regarding cost and time complexity. To establish a dependable security and privacy framework for e-Health solutions, it is imperative that all security challenges are thoroughly addressed.

2.5.1 Survivability of systems

Current frameworks for survivability tend to be highly specialized, tailored to particular applications or domains. They address challenges related to the endurance of specific systems and find application in designated fields. A multitude of survivability frameworks has been articulated within the existing literature. A select few are referenced here. Knight et al. examine the complexities surrounding survivability architectures, aiming to bolster the resilience of critical information systems. Their framework allows for the reconfiguration of an application in the event of an error. Vinko D (2023) presents a soft meddle-proofing scheme aimed at enhancing the physical survivability of wireless sensor nodes, addressing concerns related to physical tampering and the manipulation of sensor programs. The concept of system survivability encompasses the infrastructure of domain addressing systems, the sustainability of operations, and the principles of risk management. The relevance of these concepts has intensified in contemporary discourse, as the global landscape grapples with economic and political instabilities arising from conflict, climate change, inflation, societal distress, and the repercussions of the COVID-19 pandemic

(Haigneau et al., 2022). The Framework assesses the integrity of the program within each sensor device, referred to as program integrity verification (PIV). Ibrahim (2019) introduces a software-based memory attestation technique aimed at addressing the challenges of securing sensor devices and enhancing their tamper resistance, thereby ensuring their resilience against various forms of attack. Yong Yin (2019) examines the resilience of extensive and diverse information systems. Their research examines the critical matter of survivability in the context of physical assaults that compromise links and nodes within multi-network systems. The ultimate objective is to bolster essential services during a significant assault by optimizing the utilization of network resources and reducing network congestion to the greatest extent possible. (Jean-Paul A. Yaacoub, 2023) examines technologies for resilient IoT systems that ensure the reliability of information storage over time, even in the face of malicious compromises affecting a portion of the storage nodes. For the attainment of survivability, IoT systems ought to be decentralized and disseminate information across autonomous storage nodes. Gurjar (2018) introduces a system named Forensic, which employs monitoring and reconstruction mechanisms to enhance the survivability of distributed systems while minimizing the human effort required for conducting forensic analysis. (Ron Ross, 2021) introduce SABER, a comprehensive, system-level architecture that integrates a wide range of tools aimed at enhancing system survivability. The work by Win (2019) centers on quantifying appropriate metrics to define the survivability of an intrusion-tolerant database system. This paper presents a framework that examines survivability through a distinctive lens. The emphasis lies on the essential survivability criteria for a pivotal system, viewed through the lens of the user. The natural formulation of a user's policy regarding system survivability has yet to be thoroughly examined within the current body of research. The suggested framework enables a user to delineate essential survivability variables and inference rules. It additionally offers a framework for

reasoning about user survivability requirements and tackles other significant concerns in the specification of observable and certifiable survivability requirements. The framework delved into various aspects, including the development of a survivability requirement policy, the representation and interpretation of such a policy, and the domain-dependent variables and rules that a system provider may employ in the compilation of a compliance proof, among other considerations. This is a field that has received limited scholarly attention, particularly concerning system survivability solutions that can be implemented across diverse applications and domains.

2.6 Research Gaps

This research major gap was Lack of real time visibility. Immediate awareness of attacks always needs a real-time visibility of hospitals' network and systems. The members were sensitized on real time reporting of the attacks and malicious activities.

2.7 Conceptual Framework

The conceptual framework illustrated in the figure below delineates the relationship between independent and dependent variables as informed by the literature review.

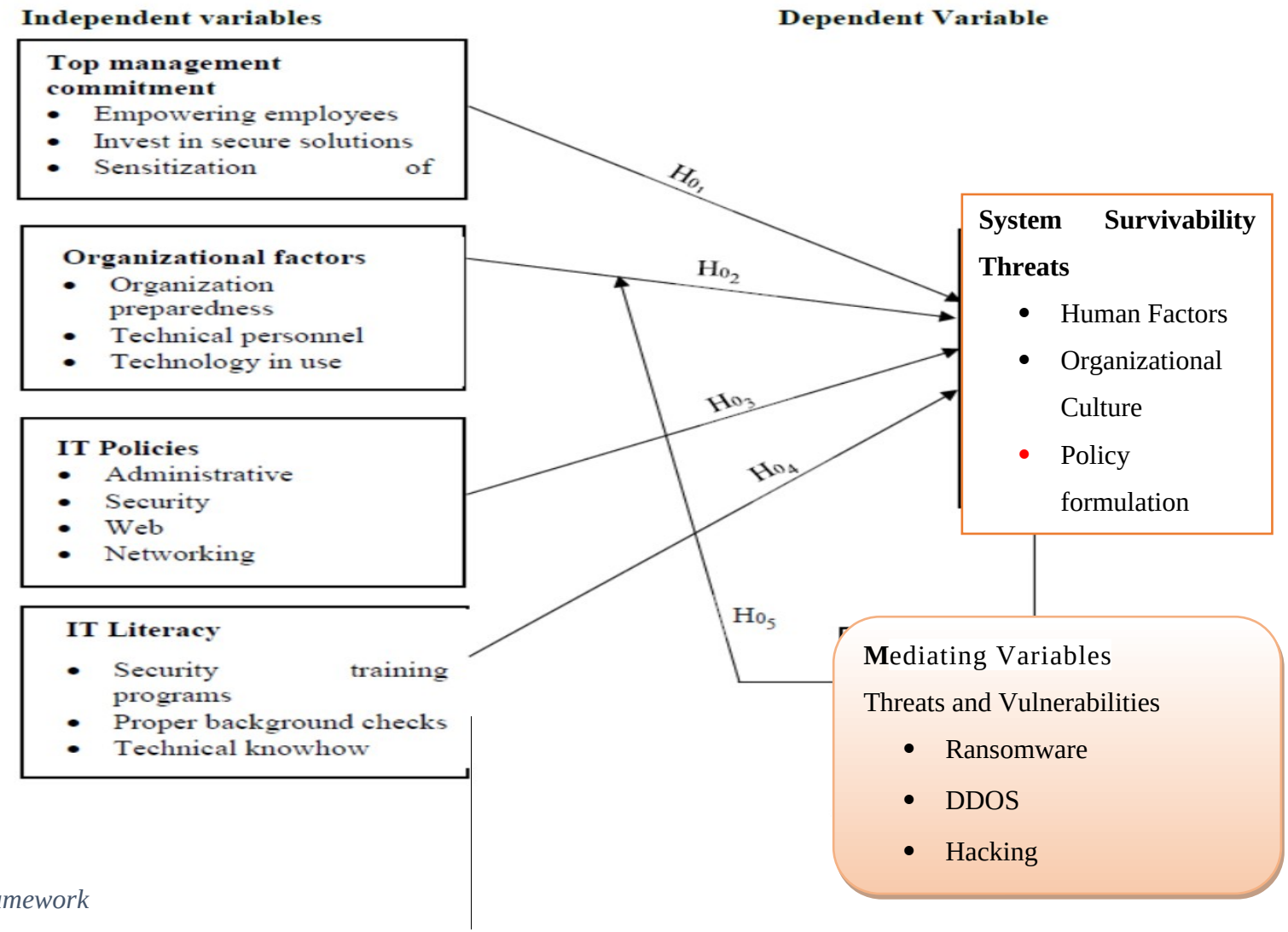


Figure 1: `

Conceptual Framework

The conceptual framework factored in the aspects below:

Top management commitment - This involves the obligation of management to enlighten their employees about the significance of systems, facilitating efficient participation, fostering a sense of ownership, and overseeing their responsibilities.

Organizational factors - Entails industry expertise on threats resulting from technology in use, organizational preparedness, and technical expertise of cybersecurity personnel.

IT policies – Entails the rules and procedures in the information technology area such as administrative, security, web-based and networking policies.

IT literacy – Involves the awareness of various information technology aspects through security and survivability training programs, proper background checks and technical knowhow.

Threats and vulnerabilities – In this study, they have been conceptualized to include ransomware, DDoS, and hacking, which are likely to affect cybersecurity and eventually system survivability in the hospital studied.

System survivability – A concept that includes numerous apparatuses meant at shielding information, networks, and organizations from unlawful abuse, normally denoted to as cyber-attacks, while ensuring that system performance remains intact even in the event of such breaches. In this study, it was looked from the human factors, organizational culture, and policy formulation aspects.

2.8 Chapter Summary

Systems survivability threats in the wake of rising exchange that comprise automated health is viewed as the most fatal risk to the economy yet to be seen. Survivability is articulated as a system's capacity to deliver critical services amidst adversities and disruptions, as well as to restore complete functionality promptly when conditions become favorable. For numerous essential systems employed in national defense, healthcare, and utilities.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Overview

The methodology of study involves a systematic with theoretical examination of the methods employed in the study of a particular subject. It encompasses the analytical examination of the methodologies and foundational principles associated with a specific domain of knowledge. It inherently includes notions such as concept, theoretical framework, stages, and both quantitative and qualitative methodologies (Khan, 2023). This chapter delineates the methodology employed to facilitate the execution of the study. The text delineates particular methodologies employed in the collection and analysis of data to fulfill the research objectives. The document encompasses a detailed framework for the collection, measurement, and analysis of data. This section primarily outlines a strategy for the selection of sources and the types of information that will be utilized to address the research objectives.

3.2 Research Design

The design of research serves as the foundational framework, acting as the cohesive force that unifies all components within a research endeavor. This document outlines the proposed research endeavor. (Dr. Akhtar, 2016). This investigation employed a research design characterized by both descriptive and inferential methodologies. As noted by McCombes (2019), descriptive research, often referred to as statistical research, serves to elucidate a phenomenon in its existing state. The authors elaborate that it serves to identify and acquire information regarding the characteristics of a

specific issue, such as a community, group, or individuals. The primary objective of descriptive research is to faithfully represent the attributes of a given situation. One might engage in a detailed examination of the operations within a manufacturing facility. The factors encompass the demographic distribution by age, the attainment of educational qualifications, the overall physical health status, and the working conditions within a factory, including aspects of health, welfare, and safety protocols. A descriptive study might focus on an individual's perspectives or attitudes regarding various subjects (McCombes, 2019).

3.3 Study area

This study was carried out in MTRH, the second largest health facility in Kenya and the largest facility in Uasin Gishu county. (Kenya harmonized health facility Assessment (MOH, Harmonized Health Facility Assessment (HHFA) Kenya 2018-2019, 2022) shows as the second largest facility in Kenya after Kenyatta National Hospital in Terms of bed capacity, and clients seeking services per day. Therefore, with expanded dependability on many systems.

3.4 Target Population

The term population denotes the complete set of individuals, occurrences, or objects that the researcher aims to examine (Thomas, 2023). The study's population comprised 2,056 staff members from the Moi Teaching and Referral Hospital, specifically those employed in the facility departments. A sample was subsequently extracted from this population.

3.4.1 Inclusion

All IT Staff, Management, Other staff and officers working in Moi Teaching referral hospital for at least the past 1year, system survivability survey targeted the IT staff who use the system, and, in this study, minors were allowed with duly signed consent form especially those who may be on learning practice in the departments at the time of the study. Above all of them should consent.

3.4.2 Exclusion Criteria

All those who did not consent.

3.5 Sample size and Sampling Technique

3.5.1 Sampling Design

Sampling involves the thorough selection of a adequate figure of factors from a people, enabling an investigation of the experiment and an estimation of its assets or traits. This understanding allows for the generalization of these assets or properties to the larger sample frame elements (https://en.wikipedia.org/wiki/Sampling_(statistics), n.d.). The process of sampling typically diminishes the duration required to finalize research endeavours. Sampling effectively reduces expenses, enhances manageability, improves accuracy, and typically reflects the characteristics of the sample population.

This research employed a convenience sampling method. Convenience sampling, as articulated by Igwenagu (2016), pertains to the gathering of data from individuals within the population who are

readily accessible to contribute such information. In this study, it was advantageous to obtain information from the available IT personnel of the Hospital.

3.5.2 Sampling Frame

A sampling frame is a specific list of specific items in your population. For this study, the researcher looked at senior IT staff and departmental heads in Moi Teaching and referral Hospital and specifically IT staff who deal daily with these crime threat cases. They also hold on to a lot of information of what happens since they constantly monitor on what is happening. This helps in giving a clear detail of what happens in terms of attacks and policies in place.

3.5.3 Sampling Technique

The sampling technique refers to the precise methodology employed in the selection of entities that constitute the sample. This study employed a convenience sampling method by the researcher. (Golzar, 2022) Convenience sampling entails the selection of participants grounded in their immediate and readily accessible availability. Students frequently favor convenience sampling because of its economical nature and straightforwardness in comparison to other sampling techniques (Golzar, 2022). Convenience sampling frequently addresses numerous limitations inherent in research methodologies. Utilizing acquaintances or relatives as part of a sample presents a more straightforward approach than seeking out unfamiliar individuals. For this study, the researcher selected IT staff due to their accessibility.

3.5.4. Sample Size

Sampling constitutes a critical aspect of statistical methodology, focusing on the identification of a subgroup of distinct studies from a broader population. This process aims to generate insights about the population in question, particularly for the purpose of making equitable generalizations of findings back to the original population from which the sample was derived (Makwana, 2023). Consequently, the participants in the study were chosen systematically according to a specific sequence. As noted by Memon (2020), the sample size is contingent upon the level of precision sought by the scholar in approximating the sample parameter at a specified assurance level; therefore, no universal guideline exists for determining sample size. A representative sample of 2056, comprising Doctors, Nurses, Clinical Officers, and IT Officers, is illustrated in the table below. The sample size was deemed both representative and thorough in addressing the study's objectives.

The selection of respondents from hospital employees was established utilizing the Fischer formula, applicable for populations exceeding 10,000 elements. This analysis was conducted utilizing a 95% confidence interval, with an alpha level set at 0.05, employing a one-tailed approach (Bostley Muyembe Asenahabi, 2023).

$$N = \mathbf{Z^2pq/\ d^2} \quad \text{……. Equation 1 (Higgins, 2001)}$$

Equation 1: Sample Size Calculation

The desired sample size was determined using the following.

Fisher et al. (1991) formulae: -

$$n = \frac{Z^2\ pq}{\mathbf{d^2}}$$

Where:

n = the desired sample size (when population is greater than 10,000).

Z = the standard normal deviation, set at 1.96, which corresponds to 95% confidence level.

= the prevalence proportion set at 0.50 in accordance with the Fisher (1991) guide.

= 1.0 – p

d = degree of accuracy desired, here set at 0.05 corresponding to the 1.96 z-statistic used in the numerator.

In substitution,

$$n = \frac{1.96^2 \times 0.5(1 - 0.5)}{0.05^2}$$ = **384**

Moi Teaching and referral hospital had a staff in post of N=2056 and since N is less than 10,000 the second formula was applied in determining the sample size. Thus: -

$$nf = \frac{n}{1 + \frac{n}{N}}$$

Where: - nf = desired sample size for a population less than 10,000.

n = desired sample size for population more than 10,000 which is 384.

N = Population which is 2**056**

Substituting, Therefore, the desired sample size, n **= 332**

The study used the stratified sampling method below to get number of clients per department and later used random sampling to get the respondents of the questionnaire from the departments.

Table 2: Sample Table (Population of the sample)

	Departments in Moi Teaching and referral Hospital	Population	Stratified Sample size
1	Theatre	126	20
2	Oncology	102	16
3	Radiology	196	32
4	Casualty	206	33
5	Pharmacy	108	17
6	IT	186	30
7	Finance	46	7
8	Transport	28	5
9	Marketing	46	7
10	Laboratory	58	9
11	Intensive Care Unit	76	12
12	Neuro Surgical	128	21
13	Medical Records	116	19
14	Human Resources	36	6
15	Mother and Baby	124	20
16	Orthopedic	168	27
17	Rehabilitation	194	31
18	Cardiology	112	18

Total	2056	332

3.6 Data Collection Methods

The research employed the collection of primary data. Primary data was collected through the administration of a questionnaire. The researcher collected data through a survey meticulously designed in alignment with the three research objectives. This questionnaire was administered by the respondents themselves and disseminated in two separate ways. One method involves manual conveyance, while the other utilizes electronic communication through a link to the online data collection tool, Google Forms.

3.6.1 Questionnaires

The questionnaires for this study were meticulously crafted in alignment with the established objectives of the research. Kothari (2019) posits that employing questionnaires for this study was beneficial due to their ease of administration and analysis, cost-effectiveness in terms of time and resources, and the convenience they offered to hospital staff, allowing them to complete the surveys at their own convenience. The meticulously crafted questionnaire was disseminated via Google Documents and Monkey Survey methods to facilitate accessibility, alongside printed hard copies circulated for completion. Respondents were allotted a two-week period to provide their feedback, accompanied by regular reminders to encourage participation.

3.7 Reliability and Validity

Preceding to the beginning of data gathering, a initial research happened. A cohort of 32 respondents, constituting approximately 10% of the overall population sample, was meticulously chosen through a straightforward random selection method grounded in the predetermined population parameters. The researcher administered the instruments to the pilot sample and subsequently scored the questions. The reliability of instruments was enhanced through the aggregation of questions that assess the same concept. The pilot questionnaires were employed in the concluding stage of data analysis.

The questionnaire was designed from the researcher's own knowledge on data and system survivability. It was subjected to validity and reliability testing by leading mock interviews with colleagues who were working or have recently worked in the health sector in Kenya and especially experience system attacks. The responses and commitments were to refine the questionnaire and structure it to meet the objectives of the research. Consequently, the research instrument was used in this study shall be valid and reliable, as the Content Validity Index (CVI) and overall Cronbach Alpha coefficient of 0.821 and 0.893 was obtained, respectively.

3.8 Research Procedure

A total of 332 questionnaires were distributed to the participants. Subsequently, both a hard copy and a digital version were disseminated to them via email. This afforded the respondents the freedom to complete the questionnaire in the manner most suitable to them. The finalized questionnaires were either meticulously selected or returned to the researcher via email. The

researcher allotted the respondents a duration of three weeks to provide their responses. Upon receipt of the completed forms, the researcher initiated the processes of data cleaning and analysis.

3.9 Data Analysis Methods

The process of analysis included both descriptive and inferential. The data was at this point coded and checked for any extremes that were later excluded (Kothari, 2019). This procedure incorporated a few phases. Information planning involved getting data and bits of knowledge from the information which we got. This is important as it helped with maintaining a strategic distance from mistaken decisions and ends. In area of erroneous information editing, I checked and adjusted data to ensure that inconsistency, illegibility, and omission are professionally managed and corrected. For descriptive data Frequency tables and percentages were used to present the findings that was obtained by use of SPPS software version 29. Correlation and simple regression analysis was used to indicate simple relationships between individual constructs with the dependent variable. For Inferential Data Analysis and model evaluation, However, before SEM modelling for the path coefficients was done, factor analysis and Confirmatory Factor Analysis (CFA) were done to uncover only the items applicable for the Framework.

3.10 Ethical Considerations

The study placed significant emphasis on ethical considerations. During the course of the research, careful consideration was given to safeguarding the individuals who provided information. The foundational elements and key aspects of the study were presented to the members through a detailed data sheet associated with the survey, ensuring their comprehension of the survey's

objectives. The data sheet also outlined matters pertaining to classification, protection, obscurity, and informed consent. Ensuring informed consent is essential for establishing robust foundational correspondence from the outset, which can reduce attrition rates and enhance the quality of the data collected. The research participants were assured that the information collected would remain confidential and that all data would be based on aggregate totals. The questionnaire was designed to avoid soliciting personal information, such as the respondent's name or the name of the association, thereby fostering anonymity. The individuals present were also briefed on the concept of the questionnaire beforehand, and they were asked to provide their informed consent by signing a form prior to the commencement of each meeting. Participants who were engaged were assigned code numbers to ensure that their identities were concealed, thereby preventing any potential recognition in the survey report. All participants were informed that they retain the right to withdraw from the study at any point prior to the final distribution of the questions or to refrain from disclosing information they are uncomfortable with.

3.11 Chapter Summary

This section has précised the study procedure that took place in the research, to take into consideration basic assessment of the discoveries, just as replication of the research in different areas if possible. This has included discussion of the materials for terms of the subjective and quantitative procedure, just as the mix of the different discoveries. The look into structure and techniques was then analyzed be considering the manners by which the research a considered for speculation and replication. This chapter has additionally talked about the different issues inside the research, including unwavering quality, legitimacy, and morals, and how these issues

influenced the examination. This chapter gives proof that the research design was deliberately built as per the examination ways of thinking being used, and that the findings of the research are established in measurable and interpretive methodologies.

CHAPTER FOUR

RESULTS, DISCUSIONS AND THEIR INTERPRETATIONS

4.1 Overview

This section exhibits the figures and data that was picked to answer the objectives on the Framework for Emerging E-health Systems Survivability threats in Kenya: Case of Moi Teaching and referral Hospital. This chapter presents results from quantitative survey grounded on the purposes of the survey.

4.2 Response Rate

The Research was conducted in (MTRH) and data collected from 18 departments. Tabe 3 below shows a combination of response rates of target respondents. 332 questionnaires were administered to the respondents, out of which 286, positively responded and filled completely, the complete questionnaires represented 86.1% positive response rate. However, 46 questionnaires were not properly completed or were not returned, and were not used for analysis, representing 13.8% non-response rate. The number of participants per strata is summarized in Table 3 below.

Table 3: Response Rate

	Departments in Moi Teaching and referral Hospital	Stratified Sample size	Positive Response (n)	Positive Response (%)	Non-response (n)	Non-response Rate (%)
1	Theatre	20	18	90%	2	10%
2	Oncology	16	14	88%	2	13%
3	Radiology	32	27	84%	5	16%
4	Casualty	33	26	79%	7	21%
5	Pharmacy	17	15	88%	2	12%
6	IT	32	32	100%	0	0%
7	Finance	7	5	71%	2	29%
8	Transport	5	2	40%	3	60%
9	Marketing	7	6	86%	1	14%
10	Laboratory	9	7	78%	2	22%
11	Intensive Care Unit	12	10	83%	2	17%
12	Neuro Surgical	21	18	86%	3	14%
13	Medical Records	19	16	84%	3	16%
14	Human Resources	6	4	67%	2	33%
15	Mother & Baby	20	18	90%	2	10%
16	Orthopedic	27	24	89%	3	11%
17	Rehabilitation	31	28	90%	3	10%
18	Cardiology	18	16	89%	2	11%
	Total	332	286	86%	46	14%

4.3 Demographic Information

The study obtained the general demographics of the respondents who participated in the study. The demographics sought from the respondents included their gender, age bracket, highest level of education achieved and years of working experience. The subsequent sub-sections present the results Noticed.

4.3.1 Gender of Participants

The respondents were asked to indicate their gender. The findings obtained show that 56% of the respondents in Hospital were male while 44% were Female. The findings indicate that males have a slightly greater ratio of females to males, but the representation is reasonable in both genders. Figure 3 shows these results.

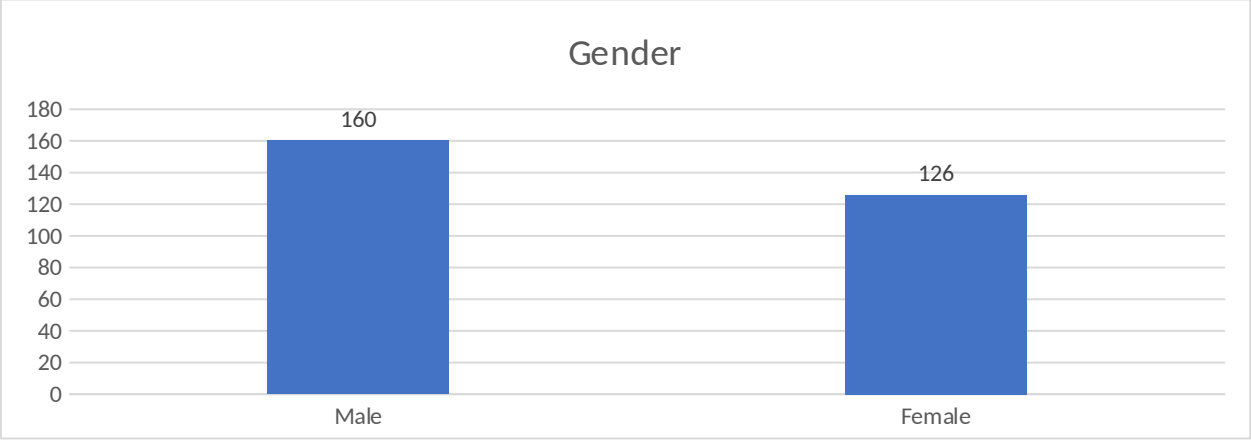


Figure 2: Gender of Participants

4.3.2 Age of Participants

The respondents were asked to indicate their age bracket. The results show that (46%) were aged 29-39 years, 37% were aged 18-28 years, 12% were matured 40-49 ages then 6% were matured 50 or more years. The findings indicate a young working force in Hospital as to compared to their older counterparts as shown Figure 4.

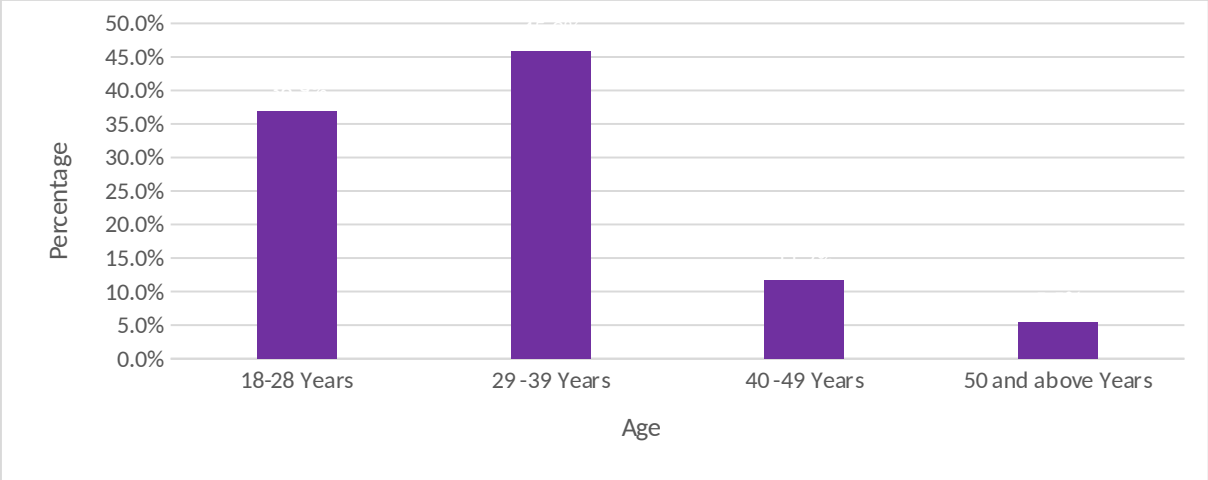


Figure 3:Age of Participants

4.3.3 Highest Level of Education of Participants

The respondents were inquired to specify the highest educational qualification they had attained. The findings show that 55.9% of the respondents had attained university bachelor's degree, 21.6% had attained Diploma level, 13.5% had a master's degree, 7.2% had attained secondary education and 1.8% had attained a Doctorate degree. The findings clearly indicate a learned workforce in Hospital. Figure 5 shows these results.

Highest Education Level of Respondents

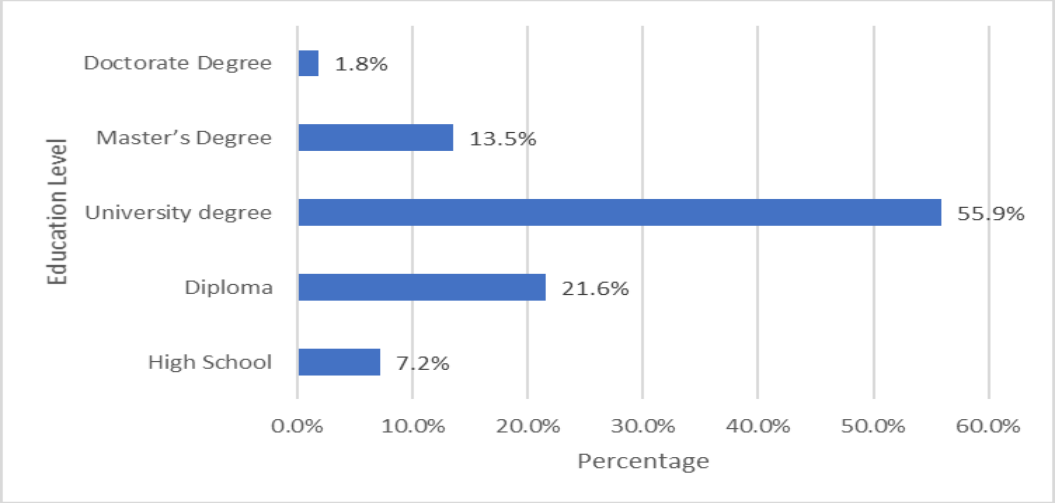


Figure 4: Highest Education Level of Respondents

4.3.4 Years of Experience of Participants

The respondents were requested to suggest how lengthy they had worked in the hospital. The results show that those who had worked for 3-5 years had the highest responses (49%), those who had worked for 1-2 years formed 24%, those who had worked for 2-3 years formed 12% while the least had worked for less than one year (5%). The responses indicate relatively low experience working in the hospital. Figure 6 shows these results.

Pie Chart Years of Experience of Participants

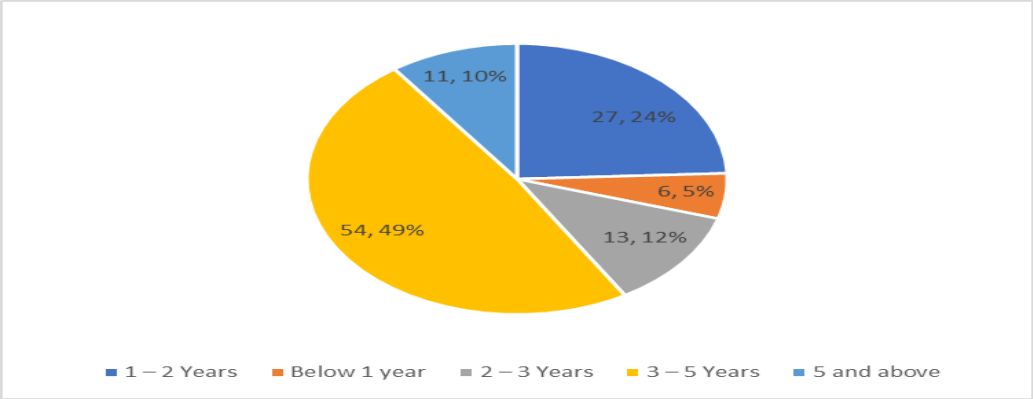


Figure 5:Years of Experience of respondents.

4.4 Findings Based on Objectives

The study first wanted to regulate if the participants had been a target of security crime and survivability attacks before. The findings indicate that 30% of the participants had stayed a target 2-5 times, 28% had been a target more than 5 times, 15% had been a target once, 11% never been a target of the attacks, while 16% of the participants had no response. The results are shown in Table 4 below.

Table 4: Number of times been a victim of system security and crime.

Response	Frequency	Percent
Never	32	11%
1 time	42	15%
2-5 times	86	30%
More than 5 times	80	28%
Non-Response	46	16%
Total Response	240	100

The research additionally aimed to assess the level of safety perceived by the participants while engaging in online activities. The results show that 35.5% of the people who took part did not feel safe, 30% did, 26.7% did, and 8% did not know. Table 5 below presents the results.

Table 5: Safety while online

Response	Frequency	Percent
Not safe	102	36%
Very safe	86	30%
Safe	76	27%
Non-Response	22	8%
Total Response	264.00	100

The research additionally aimed to ascertain whether the participants perceived any threats to their devices. The findings indicate that 39% encountered auto-generated emails in their inbox, 30% faced the publication of obscure content on their profiles, 25% dealt with Trojan or malware incidents, and an additional 3% experienced breaches involving confidential reports or information. Table 6 presents the findings of this analysis.

Table 6: Threats Experienced

Response	Frequency	Percent
Trojan or malware	72	25%
Auto generated mails to your inbox	112	39%
Publishing obscure material on your profiles	86	30%
Confidential reports/information being hacked	10	3%
Nonresponse	6	2%
Total	282.00	100

The study aimed to ascertain the respondents' perspectives on diverse facets of threats and vulnerabilities, utilizing a Likert scale for measurement. The research revealed that the participants concurred with all the statements presented to them, as detailed below: There exists a significant probability of being targeted by a ransomware attack (60.49%), a DDoS attack (56.9%), or a hacking attempt (55.24%). Additionally, threats are systematically identified and documented (29.3%), while the network is under continuous surveillance to detect potential security events (25.5%). Furthermore, the physical environment is also monitored for potential security incidents (38.81%). The findings are delineated in Table 7

Table 7: Evocative Statistics on Threats and Vulnerabilities

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It is possible for me to become a target of a ransomware attack.	f	13	15	41	44	173
	%	4.55%	5.24%	14.34%	15.38%	60.49%
I may become a target of a distributed denial-of-service attack.	f	2	13	64	44	163
	%	0.70%	4.55%	22.38%	15.38%	56.99%
I may be susceptible to a hacking attack.	f	5	2	21	158	100
	%	1.75%	0.70%	7.34%	55.24%	34.97%
Potential threats are recognized and meticulously recorded.	f	44	30	67	85	60
	%	15.38%	10.49%	23.43%	29.72%	20.98%
The network is monitored to detect potential security events for system	f	23	71	64	73	55
	%	8.04%	24.83%	22.38%	25.52%	19.23%

Survivability						
The physical environment is scrutinized to identify potential system survivability incidents.	f	36	54	31	111	54
	%	12.59%	18.88%	10.84%	38.81%	18.88%

4.4.1 Top Management Commitment

The research aimed to ascertain the perspectives of the respondents regarding the dedication of top management within the hospital setting. The observed findings reveal that a important share of sample (40.56%) concurred that the top management effectively communicates the significance of system survivability and related activities, yielding a mean of 3.36 and a standard deviation of 1.271. The considerable standard deviation indicates a significant diversity of opinions among the respondents regarding the statement. A majority of respondents concurred with the following assertions: The upper management facilitates my involvement in security and system survivability issues (38.41%), the management assumes responsibility for overseeing matters related to system survivability (33.22%), the upper management allocates resources towards solutions that are advantageous for all (31.47%), and senior management extends support to all employees who identify potential security-related concerns (29.72%). Nonetheless, the respondents expressed dissent regarding the extent of active involvement by top management in overseeing the performance of system survivability, with a notable 23.43% indicating disagreement. The results are presented in Table 8.

Table 8: Descriptive Statistics on Top Management Commitment

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The top leadership communicates to me the significance of security and system survivability initiatives.	**f**	28	59	31	116	52
	%	9.79%	20.63%	10.84%	40.56 %	18.18%
The top management facilitates my involvement in matters concerning Security and Survivability.	**f**	26	47	61	113	39
	%	9.09%	16.43%	21.33%	39.51 %	13.64%
The management assumes responsibility for overseeing matters related to security and survivability.	**f**	29	69	95	49	44
	%	10.14%	24.13%	33.22%	17.13 %	15.38%
The top management allocates resources towards initiatives that serve the collective good.	**f**	23	34	90	101	38
	%	8.04%	11.89%	31.47%	35.31 %	13.29%
The top management engages in the oversight of the effectiveness of Security and Survivability initiatives.	**f**	41	60	85	72	28
	%	14.34%	20.98%	29.72%	25.17 %	9.79%
All employees who suspect issues related to Security and Survivability receive the support of senior management.	**f**	44	49	31	95	67
	%	15.38 %	17.13%	10.84 %	33.22%	23.43 %

4.4.2 Organizational Factors

The study first sought to determine the frequency by which system survivability methods got reviewed in the hospital. The results indicate that 42.5% of participants reported that survivability methods were reviewed following an incident, 33.6% stated they were reviewed on an annual basis, 19.1% noted that reviews occurred less frequently, while 5% did not respond, as illustrated.

Table *9*: Frequency of System Survivability attacks prevention approaches evaluation.

Response	Frequency	Percent
Yearly	96	34%
Less often	54	19%
Following an occurrence	122	43%
Nonresponse	14	5%
Valid Total Responses	**272**	**100**

The participants were additionally requested to specify the individuals accountable for the evaluation of strategies aimed at preventing attacks and facilitating recovery. The findings reveal that 42% of respondents attributed the responsibility to the CEO, 31.8% identified the internal audit committees, 24% assigned it to external auditors, while 2% did not provide a response, as detailed below.

Table 10: Person responsible for carrying System survivability and attack prevention methods review.

Response	Frequency	Percent
C.E.O	**121**	**42%**
Internal Audit committee	**92**	**32%**
External Auditors	**68**	**24%**
Nonresponse	5	2%
Valid Total Responses	281	100%

The study employed a Likert scale to gather the respondents' perspectives on several dimensions of organizational components. The research revealed that the participants concurred with all assertions regarding the presence of organizational factors as outlined below: The organization designates resources to teams focused on system security (40.56%), ensuring that the costs associated with the systems in place contribute to minimal stability and security-related losses or issues (58.74%). Organization safety is integrated into the organization's continuing-term approaches (62.24%), and the organizational construct promotes staff to express their perspectives on enhancing system security (50.35%). Information involving organization safety is prioritized and engages all relevant parties (59.79%), and there is a prompt response to any attempts to compromise the systems (63.99%).

Table 11: Shows the descriptive statistics on organizational factors.

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The organization designates resources to teams engaged in the domains of system security and survivability.	**f**	10	11	116	54	95
	%	3.50%	3.85%	40.56%	18.88%	33.22%
The expenses associated with the implemented systems guarantee that losses and issues pertaining to security and system survivability remain negligible.	**f**	26	5	33	54	168
	%	9.09%	1.75%	11.54%	18.88%	58.74%
The institution incorporates system survivability within its overarching long-term strategies.	**f**	10	26	178	67	5
	%	3.50%	9.09%	62.24%	23.43%	1.75%
The organizational structure enables employees to express their perspectives on enhancing the resilience of systems.	**f**	23	0	49	70	144
	%	8.04%	0.00%	17.13%	24.48%	50.35%
Discourse pertaining to the survivability of the system is of paramount importance and necessitates the involvement of all relevant stakeholders.	**f**	5	2	59	49	171
	%	1.75%	0.70%	20.63%	17.13%	59.79%
A prompt reaction occurs whenever there is an endeavor to compromise the systems.	**f**	10	0	39	54	183
	%	3.50%	0.00%	13.64%	18.88%	63.99%

4.4.3 IT Policies

The analysis of IT policies reveals a consensus among participants regarding the existence of a security policy within the Hospital that effectively addresses system and survivability security concerns (43.36%). Furthermore, the management policies emphasize the prioritization of system security (37.7%). The organization has established guidelines governing remote access to information via mobile devices and the internet (37.06%), as well as policies pertaining to the utilization of all technologies introduced within the institution (37.76%). Additionally, there exists a system management policy that tackles threats such as viruses, user errors, and software errors (31.47%), and it is noted that policies regarding background checks for prospective employees are actively implemented (38.81%). The results are presented in Table 12.

Table 12: Expressive Statistics on IT Policies

		Strongly Disagree	Disagree	Neutral al	Agree	Strongly Agree
The organization has established a System Survivability Policy that comprehensively addresses security concerns.	**f**	36	34	23	124	69
	%	12.59%	11.89%	8.04%	43.36%	24.13%
The established management policies emphasize the importance of system security and resilience.	**f**	31	31	42	108	74
	%	10.84%	10.84%	14.69%	37.76%	25.87%
The organization has established protocols governing the remote access of information using mobile devices and internet	**f**	64	28	16	72	106
	%	22.38%	9.79%	5.59%	25.17%	37.06%
The organization maintains a set of policies governing the utilization of each technology implemented within the institution.	**f**	36	44	108	36	62
	%	12.59%	15.38%	37.76%	12.59%	21.68%
A system executive policy lives that addresses threats such as viruses, user errors, and package errors.	**f**	57	26	51	90	62
	%	19.93%	9.09%	17.83%	31.47%	21.68%
The institution implements policies regarding background checks prior to the employment of individuals.	**f**	49	31	23	111	72

4.4.4 IT Literacy

The study initially aimed to ascertain the types of technology and software utilized within the hospital, grounded in the context of IT literacy. The research indicated that 40.5% of respondents employed filtering software, while 56.8% utilized firewalls. Keyword safeguard existed was

adopted by 60.4%, and constant reviewing was observed by 40.5%. Additionally, 64.9% implemented virus protection, and 34.2% engaged in two-factor authentication. The conclusions are showed in Table 13.

Table 13: System security technology/software used.

		Yes	**No**
Filtering software	f	45	66
	%	40.5%	59.5%
Firewalls	f	63	48
	%	56.8%	43.2%
Password protection	f	67	44
	%	60.4%	39.6%
Continuous auditing	f	45	66
	%	40.5%	59.5%
Virus protection	f	72	39
	%	64.9%	35.1%
Two Factor authentication	f	38	73
	%	34.2%	65.8%

The investigation also utilized Likert scale items to measure the samples size views on diverse views of IT literacy. The research determined that the respondents agreed to the following statements: I have basic IT skills to determine and respond to system security threat (36.71%), staff are qualified on apparatuses of information in situation they intellect a security related incident (28.67%), safety parts and tasks are fit identified by all employees (29.67%), and I have sufficient knowledge on system survivability (29.72%). However, the respondents disagreed that system survivability and security training programs are done on all staff (35.31%) and there are constant familiarity programs in place on system survivability for all staffs (25.17%). And Lastly Sufficient Knowledge on system survivability at (33.22%) The findings are presented in Table 14.

Table 14: Evocative Statistics on IT Literacy

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I possess basic IT skills to determine and respond to a security threat	f	46	62	24	105	49
	%	16.08%	21.68%	8.39%	36.71%	17.13%
System survivability training programs are offered to all employees	f	67	56	26	82	55
	%	23.43%	19.58%	9.09%	28.67%	19.23%
Workers are instructed on instruments of recording in situations they recognize an in system survivability incident	f	72	52	13	64	85
	%	25.17%	18.18%	4.55%	22.38%	29.72%
System Survivability roles and responsibilities are familiar to all employees	f	41	46	101	46	52
	%	14.34%	16.08%	35.31%	16.08%	18.18%
Continuous awareness program on System Survivability are available for all employees	f	72	49	46	72	46
	%	25.17%	17.13%	16.08%	25.17%	16.08%
I have sufficient knowledge on System Survivability	f	56	52	21	95	62
	%	19.58%	18.18%	7.34%	33.22%	21.68%

The research also wanted to verify if the contestants were attracted in understanding extra about system survivability. The study found that 62% of the respondents were interested in learning more about system survivability, as 36% remained not. Table 15. shows these results.

Table 15: Interest in learning more about system Survivability.

	Frequency	**Percent**
Yes	176	62%
No	102	36%
Nonresponse	8	3%
Total Valid Response	278	100

4.4.5 System Survivability

The research revealed that the participants reached a consensus on certain statements regarding system survivability, while expressing dissent on others. The participants reached a consensus on several key points: Human factors perform a decisive role in the execution of system survivability measures (49.30%), there is a regular process for the improvement or review of internal controls within the organization (52.10%), and the formulation of policies is vital for the effectiveness of system survivability measures (27.97%). The participants expressed dissent regarding the notion that risk management is adequately implemented to guarantee effective system survivability measures (35.31%), and they indicated that system survivability monitoring is consistently conducted within the organization (71.33%). The findings are delineated in Table 16.

Table 16: Factual Statistics on System Survivability

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Human factors are used in ensuring security and survivability measures are put in place	**F**	26	23	44	52	141
	%	9.09%	8.04%	15.38%	18.18 %	49.30 %
Improvement or review of internal controls is regularly done in the organization	**F**	13	18	54	52	149
	%	4.55%	6.29%	18.88%	18.18 %	52.10 %
Policy formulation is important in ensuring security and survivability measures are effective	**F**	13	18	10	165	80
	%	4.55%	6.29%	3.50%	57.69 %	27.97 %
Risk management is done in ensuring effective system survivability measures	**F**	101	18	52	69	46
	%	35.31%	6.29%	18.18%	24.13 %	16.08 %
Security and survivability monitoring is always done in the organization	**F**	0	204	33	26	23
	%	0.00%	71.33%	11.54%	9.09 %	8.04%

4.5 Correlation Analysis

The research examined the relationship between the independent variables and the survivability of systems within a hospital context. The findings indicate that each factor exhibits a noteworthy and affirmative correlation with system security and survivability within the hospital context, as

evidenced by all p values being below 0.05. The commitment of top management exerts a moderate influence on system survivability (r = .338, p = .000). In contrast, organizational factors demonstrate a strong influence on system survivability (r = .604, p = .000). IT policies, however, show a weak influence on system survivability (r = .209, p = .028), while IT literacy reveals a strong influence on system survivability (r = .642, p = .000). Table 17 presents the correlation matrix.

Table 17: Correlation Matrix

		Systems Survivability	Top Management Commitment	Organizational Factors	IT Policies	IT Literacy
System Survivability	Pearson Correlation	1				
	Sig. (2tailed)					
Top Management Commitment	Pearson Correlation	.338**	1			
	Sig. (2tailed)	.000				
Organizational Factors	Pearson Correlation	.604**	.279**	1		
	Sig. (2tailed)	.000	.003			
IT Policies	Pearson Correlation	.209*	.745**	.289**	1	
	Sig. (2tailed)	.028	.000	.002		
IT Literacy	Pearson Correlation	.642**	.144*	.259**	.946**	1
	Sig. (2tailed)	.000	.032	.006	.006	

**. Correlation is noteworthy at the 0.01 level (2-tailed).
*. Correlation is noteworthy at the 0.05 level (2-tailed).

4.6 Regression Analysis

This is conducted when it is posited that a singular independent variable or a collection of independent variables influences a particular dependent variable. This study employed simple linear regression analysis to examine the influence of individual constructs on system survivability

within a hospital setting. The findings indicate that all the factors exhibit a significant and positive correlation with system survivability. The commitment of top management (p = .000), organizational factors (p = .000), IT policies (p = .028), and IT literacy (p = .000) all demonstrate a significant impact on system survivability within hospitals. The findings are encapsulated in Table 18.

Table 18: Regression Analysis

Independent Variable	**R**	**R^2**	**Significance (*p* value)**
Top Management Commitment	.338	.115	.000
Organizational Factors	.604	.365	.000
IT Policies	.209	.044	.028
IT Literacy	.642	.412	.000
Overall	.813	.660	.000

Dependent Variable: **System Survivability**

The findings further indicate that the t values consistently exceed 1.96 when evaluated at a 95% confidence level. The commitment of top management (t = 3.755), organizational factors (t = 7.911), IT policies (t = 2.231), and IT literacy (t = 8.743) all demonstrate a significant impact on the survivability of systems within the hospital context, as detailed below.

Table 19:Summary of Regression Coefficients

	Constant	Unstandardized coefficients		Standardized coefficients	*t* value	Significance (*p* value)
		B	Std. Error	Beta		
Top Management Commitment	1.988	.384	.102	.338	3.755	.000
Organizational Factors	1.306	.556	.070	.604	7.911	.000
IT Policies	2.542	.224	.101	.209	2.231	.028
IT Literacy	2.100	.425	.049	.642	8.743	.000

Dependent Variable: System Survivability

4.7 Discussion

This section elucidates the findings regarding the framework for system survivability, particularly in addressing the challenges of survivability and security within Kenya's health sector, alongside the emerging threats and vulnerabilities that it faces. The organization of this section is informed by the study variables. This chapter engages in a discourse regarding the relationship between the findings and the established literature, as well as insights derived from empirical investigations.

4.7.1 Emerging Threats and Vulnerabilities in the Health Facilities

The study revealed that numerous respondents had experienced multiple attacks. The attacks encompassed the generation of automated emails, the dissemination of obscure content on user profiles, the deployment of Trojans or malware, and the unauthorized access to confidential reports and information. Moreover, there were instances of ransomware attacks, DDoS attacks, and hacking incidents. In accordance with these observations, several challenges and attacks concerning system survivability have also been identified, including breaches resulting from hacking, malware, and insider threats.

Additional domains that subjected individuals to risks encompassed engagement with phishing emails, malware incursions, misconfigured security settings, improper password practices, the misplacement of laptops, and the transmission of unencrypted emails. The documentation of these attacks has been provided by Coulter et al. (2013) and Kotz et al. (2016). The present investigation revealed that these threats and vulnerabilities had a substantial and adverse impact on the survivability of the system within the examined health facility.

4.7.2 System Survivability Threat Framework Aspects

4.7.2.1 Effect of Top Management Commitment on system survivability.

The study found that top management commitment had a moderate influence on system survivability and security ($r = .338$, $p = .000$). The results from regression analysis also confirmed correlation results that top management commitment ($t = 3.755$, $p = .000$) had a significant

influence on system survivability in Hospital. From SEM analysis, the study found that the path coefficients were positive for top management commitment with system survivability. In line with these study findings, Richardson and North (2017) found that for an organization to effectively tackle system survivability challenges, the top management should be committed towards fighting these threats and challenges. Kelpsas and Nelson (2016) found that this can be done through informing their employees of the importance of systems, make it efficient for people to participate, take ownership and manage their responsibilities. They also ought to invest in a solution that benefits everyone and finally monitor performance. These findings align with the current study findings.

4.7.3 Effect of Organizational Factors on Survivability

The study found that organizational factors had a strong influence on system survivability (r = .604, p = .000). The results from regression analysis also confirmed correlation results that organizational factor (t = 7.911, p = .000) showed a significant influence on system survivability in Hospital. From SEM analysis, the study found that the path coefficients were positive for organizational factors with system survivability. Agreeing with these findings, Lakshmanan (2019) also found that organizational resources are important survivability whereby organizations that lack industry expertise on security resulting from a general lack of technology and the prohibitive expense of system security personnel are more likely to be affected by system survivability attacks and challenges. In addition, factors such as accessibility and decrease in cost of security measures has about momentous changes in the health sector in general. The findings by Bambery *et al*. (2018) also agree that with falling costs and rising availability and implementation, system survivability will have an increasingly vital role in healthcare systems in upcoming years.

However, there are instances where organizational factors have been found to be lacking, such as in Smith and Koppel (2014) who identified 45 scenarios in which the technology infrastructure failed to provide accurate support to any clinician models. Therefore, factors such as information and communication technology are important in ensuring system survivability is ensured in hospitals.

4.7.4 Effect of IT Policies on System Survivability and security

The study found that IT policies had a weak influence on system survivability (r = .209, p = .028). The results from regression analysis also confirmed correlation results that IT policies (t = 2.231, p = .028) had a significant influence on system survivability in Hospital. From SEM analysis, the study found that the path coefficients were, however, negative for IT policies with system survivability. Based on these findings, similar findings have been posited by studies such as Lye (2005), Wu (2010) and Alpcan (2006) who found that lack of government policies contributed to the variety of criminal activity, which can be committed with or against information systems. Therefore, to achieve a completely reliable security solution, the decision made by one component needs to be allowed to consider the policies of all the other components in the network. Sunagar and Biradar (2014) also determined that lack of security policies significantly contributed to system survivability threats and challenges in organizations.

4.7.5 Effect of IT Literacy on System Survivability and security

The study found that IT literacy had a strong influence on system survivability (r = .642, p = .000). The results from regression analysis also confirmed that IT literacy (t = 8.743, p = .000) had a significant influence on system survivability in Hospital. From SEM analysis, the study found that

the path coefficients were positive IT literacy with system survivability. Similar findings have been postulated by Lakshmanan (2019) who identified IT literacy as an individual factor for improved system survivability. However, a lack of awareness and information on system security matters would lead to a negative effect on system survivability. In addition, Ayofe and Irwin (2010) also found that immediate awareness of attacks always needs a real-time visibility of an organization's network and systems, for improved security and survivability in an organization.

4.8 Chapter Summary

This chapter has elucidated the methodology employed in the analysis of the collected data utilizing the SPSS statistical tool. This chapter delineates the demographic attributes of the respondents, presents the descriptive statistics of the dataset, and conducts a correlation and regression analysis to explore the interrelations among the constructs of the study. The subsequent chapter delves into the research framework.

.

CHAPTER FIVE

FRAMEWORK DEVELOPMENT

5.1 Overview

This study sought to develop and validate a System Survivability Threat Framework For the emerging threats facing health facilities, focusing on MTRH Hospital in Eldoret. The research Framework, stipulated in chapter two under the conceptual framework section, shows the relationship between four predictor variables namely top management commitment, organizational factors, IT policies and IT literacy, the moderating variable namely threats and vulnerabilities and the dependent variable of system survivability. This chapter presents how the Framework was tested and validated using data collected during the study.

5.2 The Measurement Model Assessment

This chapter has elucidated the methodology employed in the analysis of the collected data utilizing the SPSS statistical tool. This chapter delineates the demographic attributes of the respondents, presents the descriptive statistics of the dataset, and conducts a correlation and regression analysis to explore the interrelations among the constructs of the study. The subsequent chapter delves into the research framework.

5.2.1 Validity based on Factor Analysis

The questionnaire employed a five-point Likert scale, with responses ranging from ‘strongly disagree’ (assigned a value of 1) to ‘strongly agree’ (assigned a value of 5). Factor analysis was employed to evaluate the validity of the instrument items, thereby condensing them into a smaller

set of interpretable components. The initial phase of the research aimed to assess the sufficiency of the sampling for all variables involved in the study. The research revealed a Kaiser-Meyer-Olkin (KMO) value exceeding 0.7, alongside a significant Bartlett's test for all variables examined. In particular, the commitment of top management (KMO = .817), organizational factors (KMO = .763), IT policies (KMO = .870), IT literacy (KMO = .843), threats and vulnerabilities (KMO = .759), and survivability (KMO = .899) were identified. This indicates that the sampling was sufficient for all the variables involved. The findings are delineated in Table 20.

Table 20: KMO and Bartlett's Test

Variable	**KMO and Bartlett's Test of Sphericity**		
Top management commitment	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.817
	Bartlett's Test of Sphericity	Approx. Chi-Square	283.141
		df	15
		Sig.	.000
Organizational factors	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.763
	Bartlett's Test of Sphericity	Approx. Chi-Square	282.847
		df	15
		Sig.	.000
IT Policies	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.870
	Bartlett's Test of Sphericity	Approx. Chi-Square	605.533
		df	15
		Sig.	.000
IT Literacy	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.843
	Bartlett's Test of Sphericity	Approx. Chi-Square	598.710
		df	15
		Sig.	.000
Threats and Vulnerabilities	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.759
	Bartlett's Test of Sphericity	Approx. Chi-Square	262.552
		df	15
		Sig.	.000

Survivability	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.899
	Bartlett's Test of Sphericity	Approx. Chi-Square	737.820
		df	10
		Sig.	.000

Given that the sampling was sufficient, the subsequent step involved determining the factor loadings for each individual item. A total of 35 inquiries were posed to the participants for their responses. Table 21 delineates the factor loadings and encapsulates the findings of validity testing through factor analysis for each item within the study. Factor loadings below 0.6 were excluded, whereas those exceeding 0.6 were preserved. A total of twenty-eight (28) items were retained, whereas seven (7) items were excluded. The items that were dropped include OF3, TV4, TV5, TV6, CS3, CS4, and CS5.

Table 21: Factor Analysis Loadings

Item	Component Loading	Decision
TMC1	.671	Retained
TMC2	.868	Retained
TMC3	.737	Retained
TMC4	.701	Retained
TMC5	.793	Retained
TMC6	.771	Retained
OF1	.674	Retained
OF2	.827	Retained
OF3	.202	Dropped
OF4	.874	Retained
OF5	.831	Retained
OF6	.750	Retained
ITP1	.847	Retained
ITP2	.866	Retained

ITP3	.772	Retained
ITP4	.894	Retained
ITP5	.929	Retained
ITP6	.916	Retained
ITL1	.887	Retained
ITL2	.942	Retained
ITL3	.758	Retained
ITL4	.725	Retained
ITL5	.930	Retained
ITL6	.873	Retained
TV1	.899	Retained
TV2	.784	Retained
TV3	.824	Retained
TV4	.585	Dropped
TV5	.343	Dropped
TV6	.485	Dropped
CS1	.855	Retained
CS2	.831	Retained
CS3	-.266	Dropped
CS4	-.003	Dropped
CS5	.281	Dropped

5.2.2 Confirmatory Factor Analysis

Before doing the path coefficients for the SEM model, CFA was conducted using SPSS AMOS software. Figure 7 shows that the retained factors were significant and sufficient, with loadings of more than 0.4. Therefore, they were appropriate for the SEM model. The covariances that are

positive show that the factors are moving in the same direction, while the negative ones indicate that the factors are moving in the opposite direction

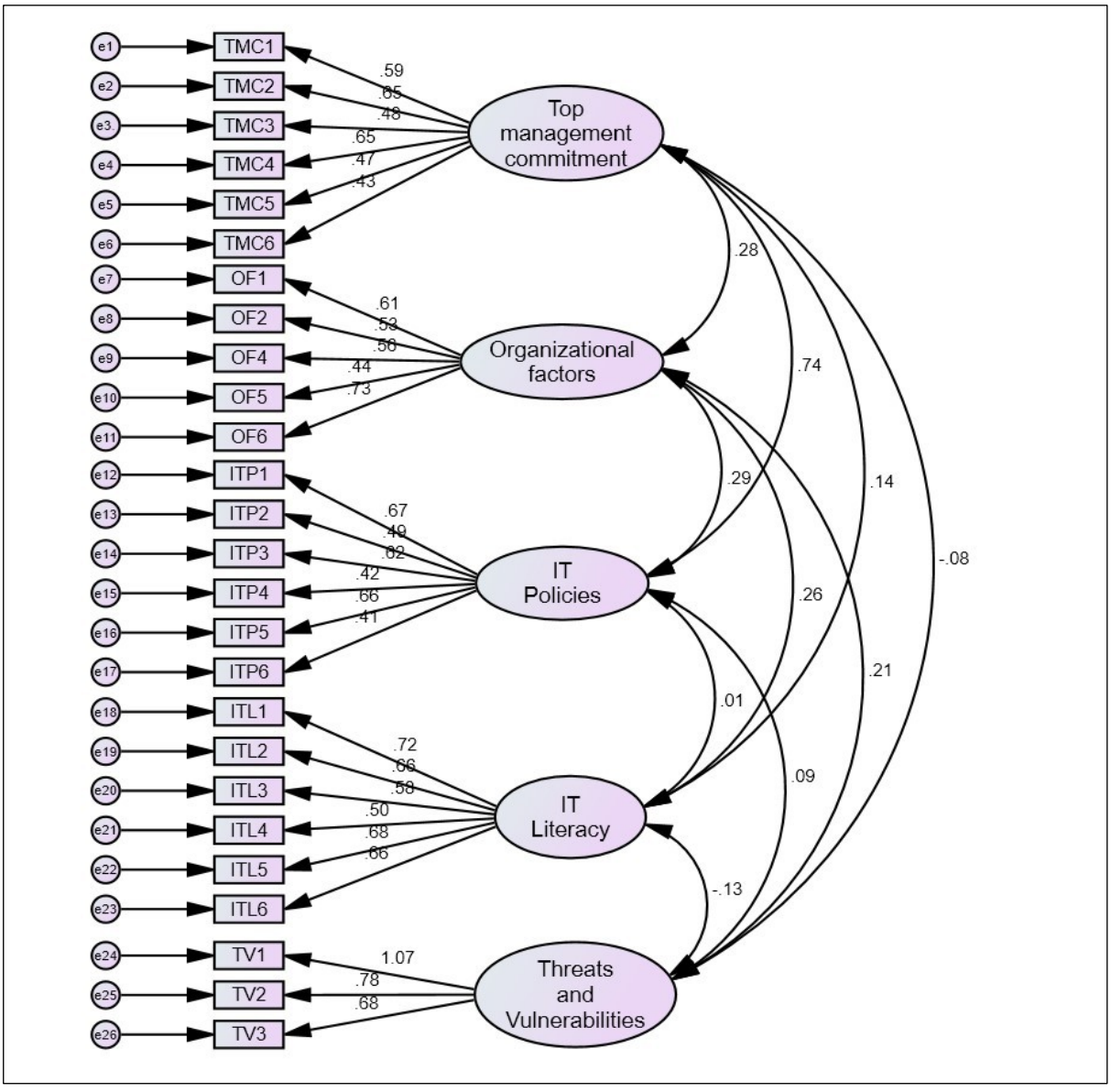


Figure 6: Confirmatory Factor Analysis

The Chi-square = 3143.493 and p = .000 were obtained, which shows the overall fit of the model. The path coefficients were also positive. In addition, all the factor loadings were well above 0.4 and therefore they were within the acceptable threshold. The findings are shown in Table 22.

Table 22: CFA Factor Loadings

			Estimates
TMC6	<---	Top management commitment	.428
TMC5	<---	Top management commitment	.471
TMC4	<---	Top management commitment	.652
TMC3	<---	Top management commitment	.483
TMC2	<---	Top management commitment	.652
TMC1	<---	Top management commitment	.595
OF6	<---	Organizational factors	.729
OF5	<---	Organizational factors	.440
OF4	<---	Organizational factors	.563
OF2	<---	Organizational factors	.533
OF1	<---	Organizational factors	.608
ITP6	<---	IT Policies	.413
ITP5	<---	IT Policies	.664
ITP4	<---	IT Policies	.420
ITP3	<---	IT Policies	.620
ITP2	<---	IT Policies	.485
ITP1	<---	IT Policies	.672
ITL6	<---	IT Literacy	.662
ITL5	<---	IT Literacy	.676
ITL4	<---	IT Literacy	.502

ITL3	<---	IT Literacy	.585
ITL2	<---	IT Literacy	.656
ITL1	<---	IT Literacy	.722
TV3	<---	Threats and Vulnerabilities	.678
TV2	<---	Threats and Vulnerabilities	.780
TV1	<---	Threats and Vulnerabilities	1.068

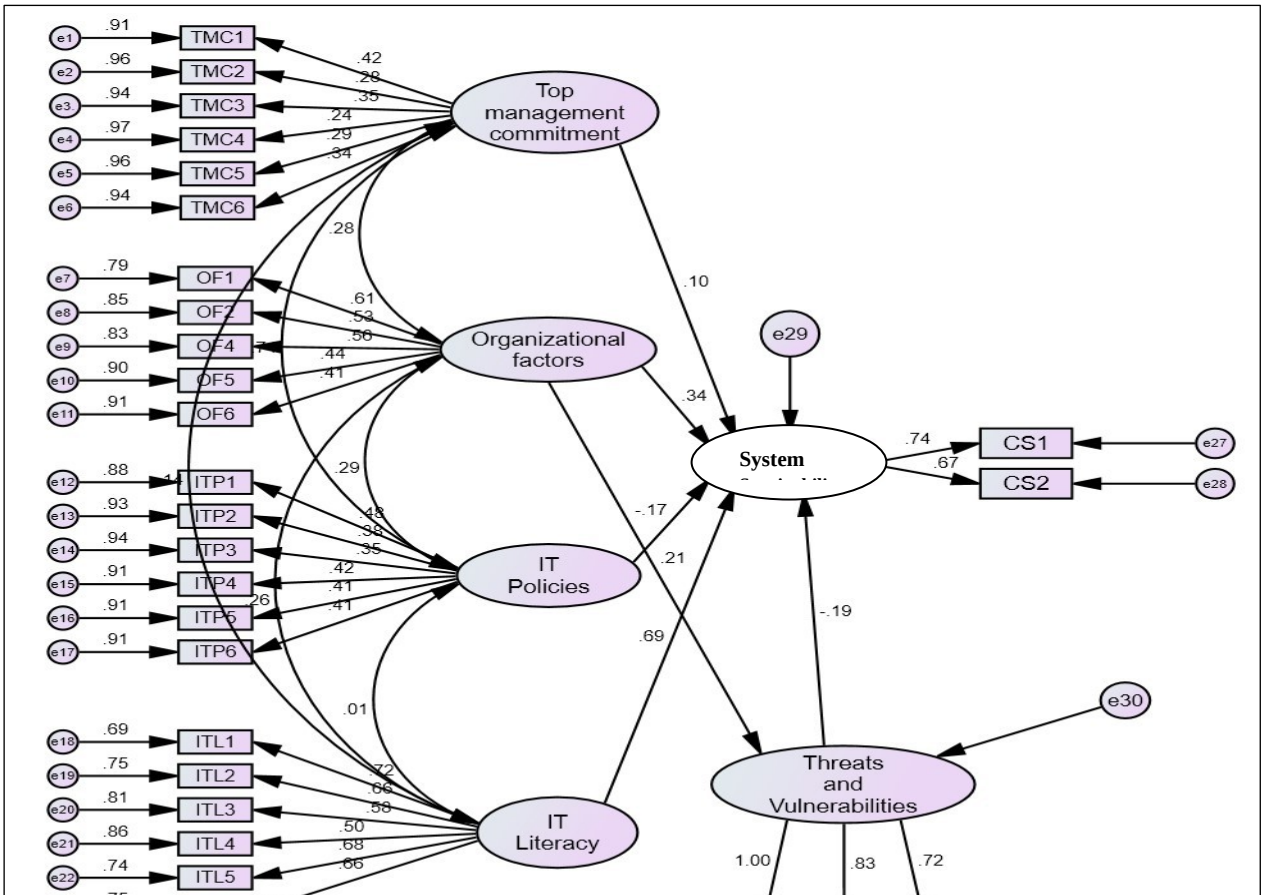
Table 23: CFA Factor Loadings

5.3 The Structural Model Assessment

5.3.1 Structural Equation Modelling Analysis

The research model developed in Figure 8 (conceptual framework section) was derived from various theories and was tested using SEM analysis based on the data obtained from the respondents. Conclusions on the influence were drawn based on the significance and critical ratios (CR) of the path coefficients. Figure 8 shows the research Framework For the study.

Figure 7: Structural Equation Modelling Analysis



The Chi-square = 2300.672 and p = .000 were obtained, which shows the overall fit of the overall research model. The table with path coefficients, standard errors, p values and Critical Ratio (CR) values was summarized as shown in **Table 23.** As shown, the path coefficients greater than 0 represent a positive relationship; and negative if the coefficient is less than 0. The significance of the relationship was determined with the p-values associated with the coefficients. The study found that the path coefficients were positive for top management commitment, organizational factors, and IT literacy with system Survivability. The paths coefficients are, however, negative for IT policies with system Survivability as well as threats and vulnerabilities with system Survivability.

Table 24: Regression Weights for the Model

			Standardized Estimate	Unstandardized Estimate	S.E.	C.R.	P Label
Threats and Vulnerabilities	<---	Organizational factors	.213	.317	.139	2.283	.022
System Survivability	<---	Top management commitment	.102	.158	.200	2.792	.019
System Survivability	<---	Organizational factors	.340	.427	.120	3.557	***
System Survivability	<---	IT Policies	-.168	.247	.190	-3.299	.001
System Survivability	<---	IT Literacy	.686	.619	.090	6.916	***
System Survivability	<---	Threats and Vulnerabilities	-.185	-.156	.074	-2.115	.034

TMC6	<---	Top management commitment	.335	.746	.200	3.735	***
TMC5	<---	Top management commitment	.292	.557	.174	3.206	.001
TMC4	<---	Top management commitment	.238	.418	.163	2.568	.010
TMC3	<---	Top management commitment	.349	.663	.170	3.909	***
TMC2	<---	Top management commitment	.275	.510	.170	3.000	.003
TMC1	<---	Top management commitment	.420	1.000			
OF6	<---	Organizational factors	.410	.515	.109	4.713	***
OF5	<---	Organizational	.440	.541	.105	5.141	***
			Standardized Estimate	Unstandardized Estimate	S.E.	C.R.	P Label
		factors					
OF4	<---	Organizational factors	.563	.861	.121	7.146	***
OF2	<---	Organizational factors	.533	.861	.130	6.603	***
OF1	<---	Organizational factors	.608	1.000			
ITP6	<---	IT Policies	.413	.880	.185	4.757	***
ITP5	<---	IT Policies	.405	.864	.186	4.651	***
ITP4	<---	IT Policies	.420	.808	.166	4.854	***
ITP3	<---	IT Policies	.349	.838	.215	3.907	***

ITP2	<---	IT Policies	.380	.732	.170	4.305	***
ITP1	<---	IT Policies	.477	1.000			
ITL6	<---	IT Literacy	.662	.900	.097	9.258	***
ITL5	<---	IT Literacy	.676	.905	.094	9.618	***
ITL4	<---	IT Literacy	.502	.593	.098	6.085	***
ITL3	<---	IT Literacy	.585	.875	.116	7.564	***
ITL2	<---	IT Literacy	.656	.901	.099	9.117	***
ITL1	<---	IT Literacy	.722	1.000			
TV3	<---	Threats and Vulnerabilities	.721	.477	.052	9.258	***
TV2	<---	Threats and Vulnerabilities	.834	.726	.062	11.731	***
TV1	<---	Threats and Vulnerabilities	1.000	1.000			
CS1	<---	Survivability	.741	1.000			
CS2	<---	System Survivability	.666	.790	.128	6.172	***

5.3.2 Reliability and Validity of the Framework

5.3.2.1 Reliability of the Framework

The Cronbach's Alpha coefficient was used for measuring the reliability of items in the SEM model in this study. Table 23 summarizes the results of the variables under the model. Cronbach

Alpha should be more than 0.70 for the model to be reliable, and all coefficients were more than 0.7, indicating that the SEM model was dependable.

Table 25: Reliability Analysis

Variable	Initial No. of Items	No. of Retained Items	Cronbach Alpha
Top management commitment	6	6	.849
Organizational factors	6	5	.851
IT Policies	6	6	.934
IT Literacy	6	6	.924
Threats and Vulnerabilities	6	3	.866
System Survivability	5	2	.770

5.3.2.2 Average Variance Extracted for Model Validity

The Average Variance Extracted (AVE) was calculated for every factor, for retained items as shown in Table 5.6. The study found that the retained items for every variable had AVE values which were more than 0.5, which means that the SEM model is valid.

Table 26: Convergent Validity based on AVE.

Variable	No. of Retained Items	AVE
Top management commitment	6	.577

Organizational factors	5	.631
IT Policies	6	.761
IT Literacy	6	.733
Threats and Vulnerabilities	3	.701
System Survivability	2	.712

5.4 The Analysis of the Direct and Indirect Effects

Structural equation modelling was used to test the five hypotheses outlined in chapter two under the conceptual framework. The significance of the relationship was determined with the *p*-values associated with the coefficients. The results of the SEM hypothesis testing are summarized in Table below.

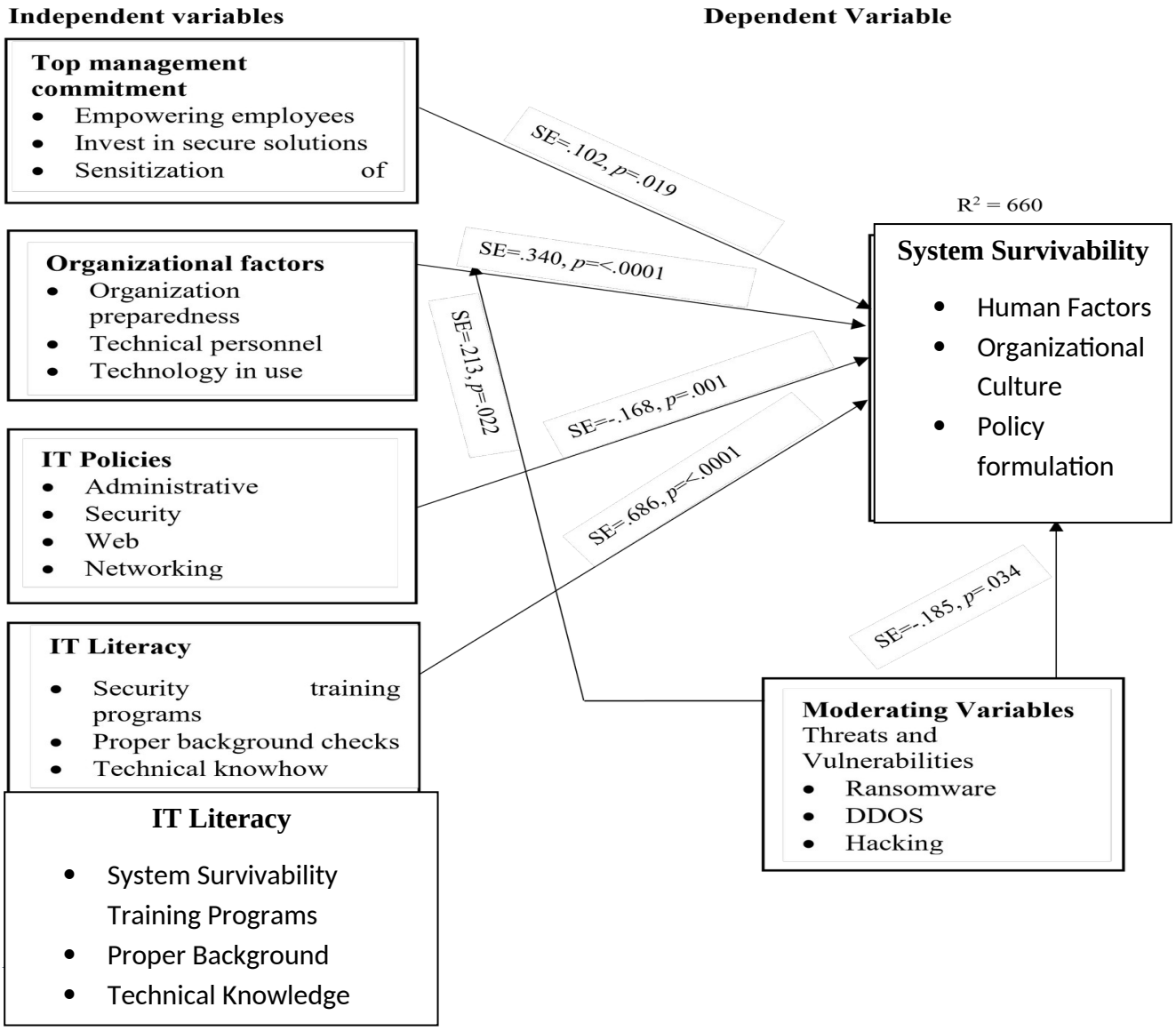
Table 27: Summary of Hypothesis Testing

Hypotheses	**Path coefficient**	**S.E.**	**C.R.**	**P Label**	**Conclusion**
H_{01} – Top management commitment does not influence security and survivability in health sector	.102	.200	2.792	.019	Alternative hypothesis accepted
H_{02} – Organization resources/factors does	.340	.120	3.557	***	Alternative hypothesis

not influence system survivability in health sector					affirmed	
H_{03} – Existing IT policies does not influence security and survivability in health sector	-.168	.190	-3.299	.001	Alternative affirmed	hypothesis
H_{04} – IT Literacy does not influence security and survivability in health sector	.686	.090	6.916	***	Alternative affirmed	hypothesis
H_{05} - Existence of challenges/ threats does not moderate the relationship between organizational individual factors and security and survivability in health.	.213	.139	2.283	.022	Alternative affirmed	hypothesis

\

A summary of the tested framework is presented in Figure 9.



5.5 Chapter Summary

In this chapter, the framework used for the study has been described, tested and validated. The analysis mechanisms to test the instruments used in the research before modelling, the path coefficients and relationships between variables has been presented. The hypotheses have also been tested in this chapter. The next chapter presents the discussion, conclusions, and recommendations.

CHAPTER SIX

SUMMARY CONCLUSION, AND RECOMMENDATIONS.

6.1 Overview

The chapter looks at the summary, discussions based on study variables, conclusions and recommendations for improvement and future research. These areas form the major subsections of this chapter.

6.2 Summary

This research aimed to develop a framework for system survivability security tailored for the implementation of autonomous systems within the healthcare sector in Kenya. The study aimed to identify the evolving threats and vulnerabilities within the healthcare sector. The analysis further examined the proliferation of various elements as a significant contributor to the increase. Consequently, the study delineated the principal threats and vulnerabilities, formulated a framework for system security and survivability, and conducted a validation process prior to advocating for its implementation within the health sector in Kenya.

The study employed a descriptive research design. The study's population comprised hospital staff members. The research concentrated on senior and intermediate IT and various departmental leaders associated with MTRH. The hospital employed a total of 2,056 personnel. This research employed a convenience sampling method. Utilizing the Yamane (1967) formula, the research encompassed a sample of 286 employees drawn from various departments. Data was collected through the administration of a questionnaire. The findings were articulated through the utilization

of frequency tables and percentages. Correlation and simple regression analysis were employed to elucidate straightforward relationships between individual constructs and the dependent variable. Structural Equation Modelling (SEM) was employed for the evaluation of the framework. The research revealed that the dedication of top management exerted a moderate effect on System survivability ($r = .338$, $p = .000$), while organizational factors demonstrated a robust influence on System survivability ($r = .604$, $p = .000$). Conversely, IT policies were found to have a minimal impact on System survivability ($r = .209$, $p = .028$), whereas IT literacy significantly affected System survivability ($r = .642$, $p = .000$). The findings from the regression analysis further validated the correlation outcomes, indicating that all factors exhibited a significant and positive relationship with System Survivability. The commitment of top management ($t = 3.755$, $p = .000$), various organizational factors ($t = 7.911$, $p = .000$), the establishment of IT policies ($t = 2.231$, $p = .028$), and the level of IT literacy ($t = 8.743$, $p = .000$) all demonstrate a significant impact on the survivability of systems within the hospital context. The SEM analysis revealed that the path coefficients exhibited positive correlations for top management commitment, organizational factors, and IT literacy in relation to security and survivability. The coefficients of the paths, however, exhibit a negative correlation concerning IT policies related to systems survivability, as well as threats and vulnerabilities associated with security.

6.3 Conclusions

Survivability is essential for any information system that delivers essential services to the nation and society. The significant importance of these systems and the grave repercussions of their failures necessitate stringent methodologies and procedures focused on systematic reasoning and

the articulation of survivability requirements from the users' viewpoint. This study introduces a novel framework that enables users to discern and articulate their survivability requirements, distinguishing it from prior research endeavors. From an engineering standpoint, requirement analysis constitutes a crucial initial phase in ensuring both security and quality assurance. The methodologies and approaches outlined in this paper are applicable across a range of contexts, requiring users to discern their application-specific survivability specification parameters in relation to the particular system being assessed. The principal contribution of this paper lies in the introduction of a framework for system survivability, aimed at enhancing decision-making processes in system development. In our forthcoming endeavors, we intend to establish a logical framework that enables a system provider to formulate proof-carrying survivability code in accordance with the user's survivability policy, utilizing high-order logic and inference rules that are contingent upon survivability considerations.

6.4 Recommendations

Based on the findings, discussions and conclusions made in the study, the following recommendations were made for improvement.

6.4.1 Threats and Vulnerabilities

Given the multitude of threats emerging from diverse sectors, the study advocates for the implementation of enhanced security and safety measures, particularly concerning the devices utilized by employees. Instances arose in which employees operated their devices devoid of any security features, thereby rendering them vulnerable to various threats. Consequently, it is

advisable to implement security measures including the utilization of anti-virus software, firewalls, Two Factor authentication, and filtering software.

6.4.2 System Survivability Threat Framework Aspects

6.4.2.1 Top Management Commitment

The study found that top management did not actively participate in monitoring the performance of system security survivability measures. The study, therefore, recommends that in addition to participation, investment to solutions that work and support to all employees who suspect security threat problems, monitoring of the performance of system survivability should be practiced in all areas. This will help ensure that the existing system security and survivability measures are practiced and implemented, and therefore lower security threats in the institutions.

6.4.2.2 Organizational Factors

The study found that system security was not fully included in the long-term overall strategies of the institution. This study, therefore, recommends that for effective security management in the hospital, System security and survivability should be given priority in the organization and should be included in the hospital strategies, whether long term or short term. This will ensure that security loopholes are closed, and safety of the organization and employee data.

6.4.2.3 IT Policies

The study recommends development of policies concerning system security that touch on various areas and departments of the organization. The existing policies should also be effectively

communicated, and the organization should ensure that they are fully implemented to avoid losses that result from insecurity and software development.

6.4.2.4 IT Literacy

The study recommends continuous awareness programs and training programs on system security and survivability for all employees. As this was found to be lacking, training and awareness creation is the first step to ensuring that employees understand the importance of ensuring syetm security measures are implemented. When they are aware, they can easily implement the strategies present and therefore system security will be improved in the Hospital.

6.4.3 Future Research

The present investigation was exclusively carried out within the confines of the Hospital, incorporating the perspectives of all personnel involved. This constrained the study's scope, particularly regarding the focal area. The research suggests that further investigations be undertaken in various hospitals, both public and private, to yield comparative findings in the same domain. Furthermore, the chosen study location was Uasin Gishu County, Kenya, which consequently constrains the scope of the research. Additional researchers may broaden their focus beyond the domestic context to examine healthcare facilities in rural regions. Additionally, an exploration of other sectors may be conducted to ascertain whether the findings align with those observed in hospitals. The study employed a methodological approach that involved testing a conceptual framework grounded in established theories through the utilization of quantitative data. Additional scholars may employ qualitative methodologies and juxtapose their results with those of the present investigation.

REFERENCES

Alabdulatif, A., Thilakarathne, N., & Kalinaki, K. (2023). *Novel Cloud Enabled Access ControlModel for Preserving the Securityand Privacy of Medical Big Data.* Basel, Switzerland: Creative Commons.

Anwar, F. &. (2020). A Comprehensive Insight into Game Theory in relevance to Cyber Security. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, 8. 189-203. 10.11591/ijeei.v8i1.1810.

avad Pool, S. A.-J. (2024). A systematic analysis of failures in protecting personal health data: A scoping review,. *Top 8 Health Care Cyber Secuirty Challenges*, 102.

Benaddi, H. I. (2022). Robust Enhancement of Intrusion Detection Systems Using Deep Reinforcement Learning and Stochastic Game. *IEEE Transactions on Vehicular Technology*. doi:10.1109/TVT.2022.3186834

BHUPENDER KUMAR, B. B. (2019). Using game theory to model DoS attack and defence. *Sådhanå*, 44:245.

Board, A. F. (2022). *A study on intersectional approaches to gender mainstreaming in adaptation-relevant interventions.*

Bostley Muyembe Asenahabi, P. A. (2023). Scientific Research Sample Size Determination. *The International Jornal of Science and Technology*.

Complete Network. (n.d.). Retrieved from https://complete.network/what-is-cyber-vandalism/.

Cremer F, S. B. (2022). Cyber risk and cybersecurity: a systematic review of data availability. . *Geneva Pap Risk Insur Issues*, 47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17.

Crime, U. N. (2022). *Digest of Cyber R organized crime.* Vienna.

Dougherty, R. (2023). *Public vs. Private Key Encryption: A Detailed Explanation.* Kiteworks.

Dr. Akhtar. (2016). Research Design.

Golzar, J. &. (2022). *Convenience Sampling* (Vol. 1). doi:10.22034/ijels.2022.162981.

Gurjar, C. (2018). *Computer forensics investigation – A case study.*

haigneau, T., Coulthard, S., Daw, T., Szaboova, L., Camfield, L., Chapin, F. I., . . . Ibrahim, M. (2022). Reconciling well-being and resilience for sustainable development. Nat. Sustain. *Google Scholar*, 5, 287–293.

Haleem A, J. M. (2021). Telemedicine for healthcare. *Capabilities, features, barriers, and applications*, doi: 10.1016/j.sintl.2021.100117. Epub 2021 Jul 24. PMID:; PMC8590973., PMCID:.

Halsey, M. N. (2022). A Cybersecurity Assessment of Health Data Ecosystems. *CYBER OPERATIONS AND RESILIENCE PROGRAM GRADUATE PROJECTS*.

He Y, A. A., & do, 2. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Apr 20; 28, 23(4):e21747. doi: 10.2196/21747.

health systems are capable of operating in real or uncontrolled conditions, o. w. (2021, August 9). High-quality health systems in the Sustainable Development Goals era: time for a revolution. Lancet Glob Health. *Erratum in: Lancet Glob Health*, 1067. doi:10.1016/S2214-109X(21)00250-3. PMID: 30196093; PMCID: PMC7734391.

https://en.wikipedia.org. (2024). *https://en.wikipedia.org/wiki/Ransomware#:~:text=(Discuss) %20Proposed%20since%20June%202024,a%20technique%20called %20cryptoviral%20extortion.*

https://en.wikipedia.org/wiki/Sampling_(statistics). (n.d.). *https://en.wikipedia.org/wiki/Sampling_(statistics)*.

https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/. (2024). *Reasons why healthcare is the biggest target for cyberattacks*. Retrieved from healthcare is the biggest target for cyberattacks.

Ibrahim, A. (2019). *securing embedded networks through secure collective attestation.* Creative Commons.

Igwenagu, C. (2016). *Fundamentals of research methodology and data collection.*

Ismail Keshta, A. O. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, Pages 177-183,.

Jagadeeswari V, S. V. (2018). A study on medical Internet of Things and Big Data in personalized healthcare system. *Health Inf Sci Syst*. doi:10.1007/s13755-018-0049-x. PMID: 30279984; PMCID: PMC6146872.

Javad Pool, S. A.-J. (2024). A systematic analysis of failures in protecting personal health data: A scoping review,. *International Jornal for Information Management*, 102719.

Jean-Paul A. Yaacoub, H. N. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations,. *Internet of Things and Cyber-Physical Systems,, 3*, 280-308. doi:https://doi.org/10.1016/j.iotcps.2023.04.002.

Khan, J. &. (2023). *Research Methodology (Methods, Approaches And Techniques).* San International Scientific Publications. doi: https://doi.org/10.59646/rmmethods/040

Klonoff. (2015). *Rsiks will continue to increase if cybersecurity has not been designed from start of the product or Project Lifecycle.*

Kothari, C. (2019). *Research Methodology: Methods and Techniques.* New Age International Publishers: New Delhi.

Kravchenko, I. (2021). Cloud computing in healthcare: . *Overview and advantages*.

Kruk ME, G. A.-D.-E. (2018). High-quality health systems in the Sustainable Development Goals era. *time for a revolution. Lancet Glob Health*, 10.1016/S2214-109X(21)00250-3. PMID: 30196093; PMCID: PMC7734391.

Lakshmanan, A. (2020). *Literature Review on the latest security & the vulnerability of the Internet of Things (IoT) & a Proposal to Overcome.*

Larkin, M. T. (2019). A Stochastic Game Theoretical Model for Cyber Security. *Air Force Institute of Technology*.

Lin HY, T. T. (2023). Identity-Based Proxy Re-Encryption Scheme Using Fog Computing and Anonymous Key Generation. Sensors (Basel). *National Library of medicine Jornal*. doi:10.3390/s23052706. PMID: 36904909; PMCID: PMC10007563.

Makwana, D. &. (2023). *Sampling Methods in Research: A Review. 7.*

McCombes, S. (2019). *Descriptive Research | Definition, Types, Methods & Examples.*

Memon, M. &.-H.-H. (2020). *Sample Size for Survey Research: Review and Recommendations* (Vol. 4). . doi:10.47263/JASEM.4(2)01.

Metty Paul, L. M. (2023). A study on privacy and security concerns,. *Digitization of healthcare sector:, 9*(4), 571-588. Retrieved from https://www.sciencedirect.com/science/article/pii/S2405959523000243

Ministry of Information, C. a. (2019). *National Information, Communications and Technology Policy.* Naribi Kenya: Goverment of Kenya.

MOH. (2018/2019). *Kenya Harmonized Health Facility Assessment.* NAIROBI: moh.

MOH. (2022). *Harmonized Health Facility Assessment (HHFA) Kenya 2018-2019.* Nairobi: moh.

Morrow, S. (2018, January). Top 10 Threats to Healthcare Security. *HEALTHCARE INFORMATION SECURITY*.

Nasibeh Zohrabi, J. S. (2019). An overview of design specifications and requirements for the MVDC shipboard power system,. *International Jornal of elctrical power and energy systems*, 680-693.

Ndlovu K, S. R. (2021, Aug 21). Interoperability opportunities and challenges in linking mhealth applications and eRecord systems: Botswana as an exemplar. *BMC Med Inform Decis Mak,* 10.1186/s12911-021-01606-7. PMID: 34419020; PMCID.

Nureni Ayofe Azeez, C. V. (2019, July 2). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal*, 97-108.

Nureni Ayofe Azeez, C. V. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis,. *Egyptian Informatics Journal, 20*(2), 97-108.

Office, N. A. (2018). *WannaCry Cyber attacks and the NHS.* Sir Amyas Morse KCB: Controller and the Auditor General.

Otukoya, T. (2024, 02 28). The securitization theor. *International Journal of Science and Research Archive*. doi:10.30574/ijsra.2024.11.1.0225

P. Stawicki, S. S. (2021). *Contemporary Developments and Perspectives in International Health Security* (Vol. 1). IntechOpen. doi:0.5772/intechopen.84766

Pan african Cybersecurity. (2022). *The evolving Cyber Security Landscape in Africa.* Kneya, Southafrica, Zambia: Liquid C2.

Picardo, E. (2023). *How Game Theory Strategy Improves Decision-Making.*

Raburu, E. (2021). A Cybersecurity Model for The Health Sector: A Case Study Of Hospitals In Nairobi, Kenya. *USIU Africa*.

Ron Ross, V. P. (2021). *Developing Cyber-Resilient Systems:* (Vol. 2). NIST Special Publication 800-160,.

Samal L, F. H. (2021). Health information technology to improve care for people with multiple chronic conditions. Health Serv Res. *Health services Reaserch Jornal*, 1006-1036.

Seh AH, Z. M. (2020, may 13). Healthcare Data Breaches:. *Insights and Implications. Healthcare (Basel).*, 133.

Serrano LP, M. K.-G. (2023). Benefits and Challenges of Remote Patient Monitoring as Perceived by Health Care Practitioners: A Systematic Review. Perm J. 20. *System Review* , 100-111.

SG., H. (2020). Electronic medical records - .. 2020 Mar;. (P. PMC7043175, Ed.) *The good, the bad and the ugly*, 68(3):417-418. doi: 10.4103/ijo.IJO_278_20. PMID: 32056991; .

Shao M, F. J. (2022, Aug). The Impact of Information and Communication Technologies (ICTs) on Health Outcomes:. *A Mediating Effect Analysis Based on Cross-National Panel Data. J Environ Public Health*. doi:10.1155/2022/2225723. PMID: 35990542; PMCID: PMC9385304.

Sivan, R., & Zukarnain, Z. (2021). Security and Privacy in Cloud-Based E-Health System. Retrieved from https://doi.org/10.3390/sym13050742

Spence, N. B. (2018). - Ransomware in Healthcare Facilities: A Harbinger of the Future? *Perspectives in health information management / AHIMA, American Health Information Management Association*.

Taylor, B. (2019). *ntersectionality 101: what is it and why is it important.*

Technology, N. I. (2023). *Artificial Intelligence Risk Management.*

Thakur, K. H. (2019). Cyber security in social media: Challenges and the way forward. IT Professional. *Cyber security in social media:*, 41-49.

Thomas, C. (2020). Introductory Chapter: Computer Security Threat. In C. T.-L. Fernández-Caramés, *{Computer Security Threats.* IntechOpen. doi:10.5772/intechopen.93041

Thomas, R. (2023). Unraveling Research Population and Sample:Understanding their role in statistical inference.

Tsai CH, E. A. (2020). Effects of Electronic Health Record Implementation and Barriers to Adoption and Use:. *A Scoping Review and Qualitative Analysis of the Content. Life*, 0.3390/life10120327. PMID: 33291615; PMCID: PMC7761950.

Tsai CH, E. A. (2020l, Dec 4). Effects of Electronic Health Record Implementation and Barriers to Adoption and Use: Life . *A Scoping Review and Qualitative Analysis of the Content.*, 10(12):327. doi: 10.3390/l.

Uwaezuoke, S. N. (2020, September 27). Strengthening health systems in Africa: The COVID-19 pandemic fallout. pp. 15-19.

Vinko D, M. K. (2023). Microcontroller-Based PUF for Identity Authentication and Tamper Resistance of Blockchain-Compliant IoT Devices. Sensors (Basel). *National Library of Medicine*, 23(15):6769. doi:10.3390/s23156769. PMID: 37571554; PMCID: PMC10422494

Wang, S. &. (2020). A Fast CP-ABE System for Cyber-Physical Security and Privacy in Mobile Healthcare Network. *IEEE Transactions on Industry Applications*, 1-1. 10.1109/TIA.2020.2969868. .

Win, S. T. (2019). Survival of an Intrusion Tolerance Database System. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, *3*(5), 1748-1751,. doi:,

Xiaotong Xu, G. W. (2020). Study on Stochastic Differential Game Model in Network Attack and Defense. *Security and Communication Networks*.

Yong Yin, Q. L. (2019). *Survivability analysis of weighted-edge attacks on complex networks with incomplete information* (Vol. 531).

APPENDICES

Appendix 1: Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **918272**

Date of Issue: **09/March/2023**

RESEARCH LICENSE

This is to Certify that Mr.. Joseph Mukhwana Simiyu of Masinde Muliro University of Science and Technology, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Uasin-Gishu on the topic: Model for Emerging E-health Systems Survivability threats in Kenya: Case of Moi Teaching and referral Hospital. for the period ending : 09/March/2024.

License No: **NACOSTI/P/23/24207**

918272

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix II: Informed Consent Form

Study Title: Framework For Emerging E-health Systems Survivability threats in Kenya: Case of Moi Teaching and referral Hospital Uasin Gishu County

Researcher: Mr. Joseph Simiyu (MCS, Student Information Technology); Masinde Muliro University of science and Technology. P.O Box 90 - 50100 Kakamega, Kenya; Mobile No: 0723467022

Why the study: This study aims to explore **Emerging E-health Systems Survivability threats in Kenya: Case of Moi Teaching and referral Hospital** Uasin Gishu County and come up with System survivability threat model.

The study will assess the emerging threats and vulnerabilities in the health facilities, develop a system survivability threat Framework For the threats facing health facilities, case of hospital, Eldoret and Evaluate the effects of the system survivability threats to the health facilities, hospital. The results will be used to formulate policies.

Procedure: By you consenting to participate, you will be asked to participate in answering the questionnaires with the only aim being to collect information to meet the purpose of this study.

Benefits: The results from the study may be used in policy making and coming up with better interventions to improve general health outcomes. Participants in the questionnaires may benefit from having their ideas and suggestions implemented in future in by facilities and the community.

Risk: There will be minimal risk to the individuals participating in this study. The primary risk of this study is therefore the loss of confidentiality of information.

Confidentiality: Information gathered in this study will be considered confidential: Filled questionnaires and consent forms will be locked in access only by the investigator, to enhance confidentiality.

Right of participants: Your participation in the current study is voluntary. You are free to either refuse to take part or to withdraw at any stage during study.

Signed Consent for Participation: I agree to participate in this study:

Sign..... Date ……...…….

Appendix III: Questionnaire

My name is Joseph Mukhwana Simiyu, a student at Masinde Muliro University of science and Technology, pursuing a master's degree in information systems technology. This questionnaire is

distributed to establish and validate a system survivability framework for adoption by the health sector in Kenya. Through your participation, the study will be able to make possible recommendations and develop a framework and practices that can be adapted by Kenyan health sector. The information you provide will be treated with confidentiality and will solemnly be used for the purpose of this study.

SECTION A: DEMOGRAPHIC INFORMATION

1. Kindly indicate your gender below

   Male

   Female

2. Please indicate your age by ticking one of the following options

   Below 18

   18 - 28

   29 - 39

   40 – 49

   50 and above

3. What is the highest level of education you have achieved?

   Primary school

   High School

   University degree

   Master's Degree

   Doctorate Degree

4. What is your department?

1	Theatre	
2	Oncology	
3	Radiology	
4	Casualty	
5	Pharmacy	

6	IT	
7	Finance	
8	Transport	
9	Marketing	
10	Laboratory	
11	Intensive Care Unit	
12	Neuro Surgical	
13	Medical Records	
14	Human Resources	
15	In-Vitro-Fertilization	
16	Orthopedic	
17	Rehabilitation	
18	Cardiology	

5. How many years of experience do you possess in Health institution?

Below 1 year

1 – 2 Years

2 – 3 Years

3 – 5 Years

5 and above

SECTION B: TOP MANAGEMENT COMMITMENT

1. To what extent do you agree with the following statements on top management commitment? **Use a scale of 1 - Strongly Disagree; 2 - Disagree; 3 - Neutral; 4- Agree; and 5 - Strongly Agree SD**

		SD	D	N	A	SA
TMC1	The top management informs me of the importance of systems survivability and safety.					
TMC2	The top management makes it easy for me to participate in					

	system survivability matters.					
TMC3	The management takes up ownership in management of responsibilities concerning systems survivability matters.					
TMC4	The top management invests in solutions that benefit everyone					
TMC5	The top management actively participates in monitoring the system performance measures					
TMC6	Senior management support in Partition and Ensure Critical Functions at Mission Completion Performance Levels					

SECTION C: ORGANIZATIONAL FACTORS

1. How often does system survivability get reviewed in your Health institution?

Quarterly

Half yearly

Annually

Less frequently

Continually

After an incidence

Other (specify) _____

2. Who is responsible for conducting the review?

C.E.O

Accountant

Internal Audit committee

External Auditors

IT officers

Outsource

Other (specify) _____

3. To what extent do you agree with the following statements concerning organizational factors?

Use a scale of 1 - Strongly Disagree; 2 - Disagree; 3 - Neutral; 4- Agree; and 5 - Strongly Agree

SD

		SD	D	N	A	SA
O1	The Hospital Board allocates resources to teams that work on system survivability and security					
O2	The cost of the systems in place ensures the system related losses/problems are minimal					
O3	System survivability is included in the long-term overall strategies of					
O4	The organization structure allows employees give their views on how to improve systems survivability.					
O5	Secure Transmissions and Communications regarding system survivability is urgent and involves all concerned parties					
O6	There is quick detection of anomalies and response wherever there is an attempt to breach the systems					

SECTION D: IT POLICIES

1. To what extent do you agree with the following statements regarding IT policies?

Use a scale of 1 - Strongly Disagree; 2 - Disagree; 3 - Neutral; 4- Agree; and 5 - Strongly Agree

		SD	D	N	A	SA
ITP1	The organization has a system survivability policy framework that Protect Information from Exploitation and guides system recovery					
ITP2	The management policies in place prioritize system survivability					
ITP3	The organization has policies on how data can be accessed					

	remotely using mobile devices and internet					
ITP4	The organization has policies concerning the use of every technology introduced in.					
ITP5	There is a system management policy that addresses threat such viruses, user errors and software errors and care of IT gadgets in the facility.					
ITP6	Policies on background checks before individuals are employed in the institution are practiced.					

SECTION E: IT LITERACY

1. Please indicate what crime technology/software you use Cybercrime software

(Circle as appropriate)

I. Filtering software Yes [] No []

II. Anti-Burglary Doors /room Yes [] No []

III. Firewalls Yes [] No []

IV. Password protection Yes [] No []

2. To what extent do you agree with the following statements regarding IT policies? **Use a scale of**

1 - Strongly Disagree; 2 - Disagree; 3 - Neutral; 4- Agree; and 5 - Strongly Agree

		SD	D	N	A	SA
ITL1	There exist continuous awareness programs in place on system survivability and security for all employees					
ITL2	System survivability and security training programs are done on all employees					
ITL3	Personnel are trained on mechanisms of reporting in case they sense of system security-related incident					
ITL4	System survivability and security roles and responsibilities are well-known by all employees					

ITL5	I have basic IT skills to determine and respond to a system security threat					
ITL6	I have sufficient knowledge on system survivability					

3. Are you interested in learning more about system survivability crimes and how to prevent it to have seamless systems and working in the Institution?

Yes

No

Other (specify) _____

SECTION F: THREATS AND VULNERABILITIES

1. How many times have you been a victim of system crimes?

Never

1 time

2-5 times

More than 5 times

2. How safe do you feel about your information, while you are online?

Very safe

Safe

Not safe

Don’t know.

3. Have you ever suffered any of these situations?

Trojan or malware

Auto generated mails to your inbox.

Publishing obscure material on your profiles.

Confidential reports/information being hacked.

Never experienced such situation.

Computers stolen.

4. Which effect did face after above situation?

Loss of information

Poor working of the systems.

Staff inability to deliver.

Confidential of data lost.

System didn't recover after the attack.

Never experienced such situation.

5. How can it be prevented from happening again?

Have policies to Guide the situations.

Continues sensitization to the staff.

Don't Know

6. To what extent do you agree with the following statements in concerning threats and vulnerabilities? **Use a scale of 1 - Strongly Disagree; 2 - Disagree; 3 - Neutral; 4- Agree; and 5 - Strongly Agree SD**

		SD	D	N	A	SA
ITL1	There exist continuous awareness programs in place on system survivability and security for all employees					
ITL2	System survivability and security training programs are done on all employees					
ITL3	Personnel are trained on mechanisms of reporting in case they sense of system security-related incident					
ITL4	System survivability and security roles and responsibilities are well-known by all employees					
ITL5	I have basic IT skills to determine and respond to a system security threat					

ITL6	I have sufficient knowledge on system survivability					

SECTION G: System Survivability and Security

7. To what extent do you agree with the following statements in concerning threats and vulnerabilities**? Use a scale of 1 - Strongly Disagree; 2 - Disagree; 3 - Neutral; 4- Agree; and 5 - Strongly Agree SD**

		SD	D	N	A	SA
CS1	Human factors are considered in ensuring system survivability measures are put in place					
CS2	Improvement or review of internal controls is regularly done in the organization to guarantee system survivability					
CS3	Policy formulation is important in ensuring system survivability measures are effective					
CS4	Risk management is done in ensuring effective system survivability measures					
CS5	System survivability monitoring is always done in the organization to Manage System Performance if Degraded by Event					
CS1	Human factors are considered in ensuring system survivability measures are put in place					