AN EXAMINATION OF THREATS AND COUNTERMEASURES RELATING TO HEALTHCARE CYBER RISKS. THE CASE OF KENYATTA NATIONAL HOSPITAL (KNH)

STEPHEN OKONGO ARIO

A Thesis Submitted to the School of Science and Technology in Partial Fulfillment for the Requirement of Degree of Master of Science in Computer Information System of Kenya Methodist University

SEPTEMBER, 2025

DECLARATION

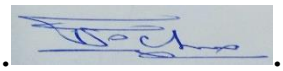
This research dissertation is my original work and has not been submitted for examination to any other university.

Signature:  **…….. Date: 26/09/2025**

Stephen Okongo Ario

CIS-3-2431-2/2022

This dissertation has been submitted for examination with our approval as the supervisor.

Signature: ……  **… Date: 26/09/ 2025**

Dr. Jecton Tocho, PhD
Department of Computer Science
Kenya Methodist University

Signature: …… Date: 26/09/ 2025

Mrs. Jenu John
Department of Computer Science
Kenya Methodist University

ABSTRACT

The increasing reliance on digital technologies in Kenya's healthcare sector has heightened the need for robust cybersecurity measures to protect sensitive patient data and ensure operational continuity. This study examined cybersecurity threats and countermeasures at Kenyatta National Hospital (KNH), the country's largest public referral hospital, to develop a contextually relevant framework for enhancing data protection and institutional resilience. Specifically, the research investigated perceived cyber risks, the influence of the Kenya Cybercrime Act, and ethical data protection practices on the effectiveness of the hospital's cybersecurity framework. Guided by the Socio-Technical Systems (STS) Theory, the study adopted a descriptive cross-sectional research design, utilizing a quantitative approach. A stratified random sample of 370 KNH staff, including ICT personnel, clinicians, and health records and admins, were surveyed using structured questionnaires, achieving a 98.6% response rate (365 valid responses). Data analysis involved descriptive statistics, correlation, and multiple regression techniques, ensuring robust insights into the relationships among key variables. Findings on cybersecurity threats revealed high perceived risks, particularly from external attacks ($M = 4.18$, $SD = 1.09$, $Var = 1.19$), device vulnerabilities ($M = 3.99$), and insider threats ($M = 3.92$). Correlation analysis showed that threats were strongly associated with the Cybercrime Act ($r = 0.602$, $p < 0.01$) and moderately with ethical guidelines ($r = 0.485$, $p < 0.01$), but insignificantly with the cybersecurity framework itself ($r = 0.055$, $p = 0.297$). Regression confirmed a significant negative coefficient for threats ($B = -0.182$, $p = 0.007$), indicating that heightened threats weaken the framework's effectiveness. Analysis of the Kenya Cybercrime Act demonstrated moderate correlations with ethical guidelines ($r = 0.539$, $p < 0.01$) and a weaker positive correlation with the cybersecurity framework ($r = 0.191$, $p < 0.01$). In regression, the Act had a positive but marginally insignificant coefficient ($B = 0.136$, $p = 0.054$; $Beta = 0.129$), suggesting that while legal provisions support cybersecurity, their influence is not yet robust. For ethical guidelines, results showed a moderate correlation with the cybersecurity framework ($r = 0.294$, $p < 0.01$). Regression identified ethical guidelines as the most influential predictor ($B = 0.303$, $p < 0.001$; $Beta = 0.309$), confirming their pivotal role in strengthening KNH's cybersecurity posture. The overall regression model was statistically significant ($F(3,361) = 14.267$, $p < 0.001$) with $R = 0.326$, $R^2 = 0.106$, and Adjusted $R^2 = 0.099$, indicating that the three predictors jointly explained about 10.6% of the variance in the hospital's cybersecurity framework. The study concludes that ethical data protection guidelines are the strongest determinant of a resilient cybersecurity framework, while rising threats undermine readiness and the Cybercrime Act contributes moderately. It recommends strengthening ethical enforcement, embedding role-based staff training, enhancing legal compliance, and allocating resources to mitigate threats. Future research should simulate incident scenarios and assess patient data literacy across hospitals.

Keywords: Cyber Threats, Cybersecurity, Data Security Framework, Ethical Data Protection, Healthcare, Kenyatta National Hospital, Kenya Cybercrime Act, Socio-Technical Systems Theory

LIST OF ABBREVIATIONS

KNH – Kenyatta National Hospital

ICT – Information and Communication Technology

GDPR - General Data Protection Regulation

NCC - National Cybersecurity Centre

HIPAA – Health Insurance Portability and Accountability Act

HER – Electronic Health Record

PHI – Patient Health Information

NIST - National Institute of Standards and Technology

DPA – Data Protection Act

KCA – Kenya Cybercrime Act

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to those who have supported and guided me throughout this research study. My deepest thanks go to my supervisors, Dr. Jecton T. Anyango and Mrs. Jenu John, for their invaluable guidance, expertise, and encouragement. Their insights and constructive feedback have been instrumental in shaping this study and ensuring its quality. I also wish to extend my appreciation to the staff and management at Kenyatta National Hospital for their cooperation and willingness to participate in the survey, which provided crucial data for this research. Finally, I am grateful to my family and friends for their continuous support and understanding throughout the course of this project.

Thank you all for your contributions and support.

DEDICATION

This thesis is dedicated to my family both in the USA and Kenya, for their unwavering support and encouragement throughout my academic journey. Their belief in my abilities and their sacrifices have been a constant source of inspiration. I also dedicate this work to the dedicated healthcare professionals at Kenyatta National Hospital, whose commitment to safeguarding patient data and improving healthcare services motivated this research. Lastly, I dedicate this thesis to all those striving to advance cybersecurity measures in healthcare settings, with the hope that this work contributes to a safer and more secure environment for patient care.

TABLE OF CONTENT

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1 Introduction

The integration of digital technologies into healthcare has transformed clinical workflows, administrative systems, and patient engagement. From electronic health records (EHRs) to telemedicine and cloud-based diagnostics, modern hospitals increasingly depend on complex information systems to enhance care delivery, data access, and coordination across departments (Obeidat et al., 2021). However, this digital transformation has introduced a parallel increase in cybersecurity threats, which are especially acute in hospital environments due to the real-time, mission-critical nature of clinical operations (Ghafur et al., 2022).

1.1.1 Threats in healthcare cyber risk

Globally, hospitals face a unique set of cyber threats distinct from those in other sectors. These include ransomware attacks that disrupt access to clinical systems, phishing attacks targeting hospital staff, breaches of medical records, malware targeting network-connected medical devices, and denial-of-service (DoS) attacks that cripple hospital portals and appointment systems (Kane & Skibinski, 2021; Kim & Yoon, 2023). For example, the 2017 WannaCry attack disrupted over 80 hospital trusts in the UK, forcing delayed treatments and emergency referrals (Martin et al., 2021). The healthcare sector's vulnerability is further intensified by factors such as legacy systems, insufficient IT investment, complex vendor ecosystems, and inadequate cybersecurity training among health professionals (Ashrafi et al., 2022).

In Sub-Saharan Africa, the adoption of digital health systems is accelerating, yet cybersecurity preparedness remains significantly underdeveloped. Public hospitals are rapidly deploying

electronic medical records (EMRs), laboratory information systems (LIS), and cloud-based patient registries, often without parallel investment in cybersecurity infrastructure or staff training (World Health Organization [WHO], 2022). A regional study by Sewanyana and Okello (2021) found that more than 70% of East African public healthcare institutions had no formal cybersecurity frameworks, and most lacked institutionalized incident reporting protocols. In countries like Uganda and Tanzania, hospitals continue to experience system downtimes and breaches attributed to weak access controls, lack of encryption, and minimal IT governance structures (Chigada & Kyobe, 2022). These issues mirror a broader challenge in the region, where cybersecurity policies are often reactive rather than proactive and are rarely contextualized to the healthcare setting.

In Kenya, the Ministry of Health has promoted digital health adoption through platforms like DHIS2, Afya Care, and integrated hospital management systems. However, national surveys have flagged cybersecurity as a neglected priority in public healthcare digitization efforts (Kimani & Wanjiru, 2023). Despite the enactment of the Kenya Cybercrime and Computer Misuse Act (2018) and the Data Protection Act (2019), implementation remains inconsistent, particularly at the institutional level. Many hospitals lack dedicated cybersecurity teams, structured staff training, or internal audits to assess compliance. Moreover, studies show that there is limited awareness among healthcare workers of their legal responsibilities under these frameworks (Mutinda & Ongus, 2020).

Kenyatta National Hospital (KNH), as the country's premier public referral and teaching hospital, has adopted various digital platforms, including EHRs, LIS, biometric patient verification, and interdepartmental system integrations. These systems have improved operational efficiency, yet they also present significant cybersecurity vulnerabilities especially where risk assessments are

infrequent and where end-user awareness is low. Preliminary observations indicate that KNH, like many public institutions, operates with limited cybersecurity-specific budget allocations, decentralized IT governance, and fragmented implementation of ethical data protection standards (Kimani & Wanjiru, 2023). While the infrastructure exists, the absence of empirical data on cyber risk awareness, legal compliance, and ethical enforcement undermines efforts to safeguard patient information and institutional integrity. These thus forms the first objective of the study which sought to examine the threats and countermeasures in healthcare cybersecurity at Kenyatta National Hospital and proposes a comprehensive, context-specific cybersecurity framework tailored for the Kenyan public health context.

1.1.2 The Legal and Policy Framework: The Role of the Kenya Cybercrime Act

In response to increasing global cyber threats, many countries have implemented legal frameworks to govern information security and data protection. For instance, the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union offer comprehensive regulatory guidelines that prioritize individual data rights, institutional accountability, and breach notification procedures (Gordon & Wright, 2020; Kshetri, 2021).

Kenya has similarly established two core legal frameworks to address cybercrime and data privacy: the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019). The former criminalizes various offenses such as unauthorized system access, computer fraud, cyber harassment, identity theft, and data interference (Republic of Kenya, 2018). The latter aligns with international standards like GDPR and defines the roles of data controllers and processors while

mandating lawful, fair, and transparent handling of personal data (Office of the Data Protection Commissioner, 2022).

However, studies show that implementation of these laws within the public health sector remains limited. According to Serianu's National Cybersecurity Report of (2020), only 17% of Kenyan public institutions have implemented structured cybersecurity programs, and only 11% of health sector organizations report regular legal compliance audits. Moreover, the Communications Authority of Kenya (2021) notes that public hospitals rarely have incident response plans or formal procedures for legal escalation in the event of a breach.

These issues are compounded by skill gaps. Research by Centre for Intellectual Property and Information Technology Law (CIPIT, 2021), and Kimani and Wanjiru (2023) confirms that most Kenyan healthcare workers are unfamiliar with the legal provisions of the Cybercrime Act and are rarely trained in how to apply them in digital health settings. This legal knowledge gap creates inconsistencies in how patient data is protected and undermines institutional accountability.

At Kenyatta National Hospital (KNH), these challenges are evident. Despite deploying advanced systems such as electronic medical records (EMRs) and laboratory information systems (LISs), the hospital does not have a dedicated legal compliance team for cybersecurity (Mutinda & Ongus, 2020). A survey by Kimani and Wanjiru (2023) found that over 60% of KNH administrative and clinical staff were unaware of how the Cybercrime Act applies to their daily tasks. There is also no publicly available documentation outlining how the hospital ensures legal conformity with either the 2018 or 2019 legislation (KNH Strategic Plan, 2018–2023).

Given KNH's scale and influence in Kenya's healthcare system, it is imperative that the Cybercrime Act is internalized not just in policy but in practice. This study, therefore, assesses how legal awareness, enforcement mechanisms, and institutional policies have evolved in light of Kenya's legal reforms. The findings aim to inform a more legally robust cybersecurity framework, tailored to the realities of KNH and similar public health institutions.

1.1.3 Ethical Data Protection in Digital Healthcare

While legal frameworks establish the parameters of data governance, ethics addresses the values underpinning how data should be handled. Ethical data protection ensures that patient information is treated with respect for privacy, confidentiality, informed consent, and autonomy, regardless of the presence of technical controls (Beauchamp & Childress, 2019). In healthcare, ethical breaches not only erode patient trust but may lead to harmful consequences, including stigmatization, discrimination, or compromised treatment outcomes (Shachar et al., 2020).

In the era of digital health, ethical concerns have expanded. The use of electronic health records (EHRs), cloud storage, biometric verification, and health data analytics introduces new risks, such as unauthorized third-party access, data commodification, and systemic surveillance without consent (Mittelstadt & Floridi, 2016; Maher & Kruger, 2022). Therefore, ethical safeguards must evolve to match the complexity of emerging technologies.

Kenya's Data Protection Act (2019) includes several ethically relevant principles such as purpose limitation, data minimization, accuracy, and accountability (Office of the Data Protection Commissioner, 2022). However, a national assessment by CIPIT (2021) reported that over 68% of public healthcare workers had no formal training in ethical data handling, and only a small minority understood key patient rights under the Act. These findings suggest that while Kenya has the

legislative tools, its ethical data governance remains weakly institutionalized in practice. Within KNH, ethical vulnerabilities are apparent in both system design and institutional culture. According to KNH's own internal evaluations (KNH Strategic Plan, 2018–2023), most departments lack formal guidelines on consent for electronic data, and there is no standardized process for controlling interdepartmental access to patient records. This often results in sensitive patient data being shared without proper authorization, especially in emergency settings where decisions are made quickly (Willis, 2015).

Moreover, digital platforms such as LIS and EMRs at KNH do not consistently implement audit trails or role-based access controls, which are critical for accountability (Kimani & Wanjiru, 2023). Mutinda and Ongus (2020) also report that KNH has not yet established a functional data ethics committee, nor does it conduct regular ethical audits of its digital systems. Given these challenges, this study examines the extent to which ethical principles of data protection have been adopted at KNH, and whether these principles are embedded in staff training, digital policy, and patient communication. By addressing this issue, the study contributes to its broader aim of building a socio-technical cybersecurity framework that is not only legally compliant but also ethically sound.

1.1.4 Kenyan Healthcare System: An Overview

Kenya's healthcare system, composed of public and private providers operating across four tiers community, primary, secondary, and tertiary continues to face systemic challenges including underfunding, staff shortages, inadequate infrastructure, and a high burden of infectious diseases (Ministry of Health, 2020; WHO, 2021). Despite government initiatives to improve access through insurance expansion and facility upgrades, rural and low-income populations often remain underserved.

Recent years have seen a growing integration of digital technologies such as electronic health records (EHRs), telemedicine, mobile health (mHealth), e-prescriptions, and mobile clinics. These tools are reshaping healthcare delivery by enhancing access, reducing operational inefficiencies, and supporting disease surveillance and maternal health (Kimani & Wanjiru, 2023; Kumar & Oyieke, 2021). However, the rapid digitalization has outpaced the sector's preparedness for cybersecurity threats, particularly in public institutions.

Cyber risks including data breaches, ransomware, and unauthorized system access are emerging as critical concerns, especially in hospitals that manage large volumes of sensitive patient data. The 2017 global WannaCry attack, which disrupted hospital services in over 99 countries, including parts of Africa, underscored the vulnerability of under-secured digital health systems (Fox-Brewster, 2017; Wong, 2017). As Kenya's digital health landscape expands, institutions like Kenyatta National Hospital (KNH) the largest public referral and teaching hospital must strengthen cybersecurity governance to protect patient data, ensure service continuity, and comply with evolving legal and ethical standards. This study is therefore situated within this broader healthcare transformation, aiming to assess cyber risks, legal implementation, and ethical data protection practices within KNH's digital infrastructure.

1.1.5 Context of the Study

Kenyatta National Hospital (KNH) is the largest teaching and referral hospital in East and Central Africa, with a capacity of 1,800 beds, 24 theatres, 22 outpatient clinics, and a staff of over 4,600 (KNH Annual Report, 2018). Established in 1901 and granted state corporation status in 1987, the hospital operates under a Board of Directors and serves as a key training partner of the University of Nairobi through a formal Memorandum of Understanding (KNH Strategic Plan, 2018–2023).

KNH manages more than 70,000 inpatients and 520,000 outpatients annually, drawing referrals from across Kenya and neighbouring countries due to its specialized care and medical expertise (Willis, 2015). Many patients bypass lower-tier facilities and self-refer, attracted by KNH's advanced diagnostic capabilities and concentration of specialists. As a result, the hospital experiences chronic overcrowding and long wait times, patients in the emergency unit often wait 7–9 hours before admission (KNH Strategic Plan, 2023). The daily patient load averages 2,000 to 3,000, straining resources and affecting service delivery. To enhance operational efficiency, KNH has adopted a range of digital technologies, including electronic health records (EHRs), laboratory information systems (LIS), biometric patient verification, and interdepartmental data-sharing platforms (Kimani & Wanjiru, 2023). These tools have improved administrative workflows and clinical documentation. However, they have also introduced significant cybersecurity vulnerabilities, particularly in the absence of centralized IT governance, regular system audits, and staff training on data protection and cyber hygiene (Mutinda & Ongus, 2020).

Given KNH's pivotal role in Kenya's public healthcare infrastructure and its advanced digital integration, it presents a critical case for investigating hospital-specific cyber threats. This study examines the extent of KNH's exposure to cybersecurity risks, assesses its compliance with Kenya's Computer Misuse and Cybercrimes Act (2018), and evaluates the integration of ethical data protection principles into hospital operations. Findings from this case helps inform a context-sensitive cybersecurity framework applicable to other public health institutions in similar environments.

1.2 Problem statement and purpose of the project

Cybersecurity is a critical determinant of healthcare performance because it directly affects the confidentiality, integrity, and availability of patient data, which in turn influences service delivery,

patient safety, and institutional trust. Globally, healthcare facilities have increasingly become prime targets of cyberattacks, with incidents of ransomware, unauthorized access, and large-scale data breaches causing operational disruptions and reputational damage (Ghafur et al., 2022). In Kenya, the rapid adoption of electronic health records, networked medical devices, and digital hospital systems has heightened exposure to cyber risks, particularly in large public institutions such as Kenyatta National Hospital (KNH).

Theoretically, the Socio-Technical Systems (STS) theory provides a basis for understanding how cybersecurity outcomes in healthcare are shaped by both technical and social factors, including infrastructure, policy, staff practices, and organizational culture (Trist & Bamforth, 1951). From a governance perspective, the Deterrence Theory and Institutional Theory also highlight the role of laws, regulations, and ethical guidelines in shaping compliance and discouraging malpractice. These perspectives underscore the importance of combining legal, ethical, technical, and human dimensions to achieve robust cybersecurity in healthcare.

Empirical studies have shown that healthcare institutions face distinct cybersecurity challenges. International research has identified common risks such as phishing, ransomware, and IoT or medical device vulnerabilities (Alami et al., 2020; Kruse et al., 2017). In the African context, Sewanyana and Okello (2021) observed weak institutional capacity in Uganda's hospitals, while Kimani and Wanjiru (2023) reported that Kenyan hospitals face persistent risks due to limited infrastructure, low staff awareness, and inadequate enforcement of data protection laws. However, most of these studies have either focused on general IT risks in developing countries or legal compliance in isolation, without holistically linking threats, legal frameworks, and ethical guidelines to hospital-level cybersecurity performance.

Despite the enactment of the Kenya Cybercrime Act (2018) and the Data Protection Act (2019), as well as the presence of ethical codes on patient data, KNH continues to face vulnerabilities. Policy implementation and enforcement remain weak, technical infrastructure is often outdated, and staff training on cybersecurity is irregular and insufficient. In addition, incident detection and response mechanisms are poorly coordinated, and inconsistencies persist in enforcing ethical principles such as confidentiality and role-based access to patient information. These issues collectively undermine KNH's capacity to safeguard sensitive health data against cyber threats.

From this perspective, three key gaps are evident. First, there is a conceptual gap, since limited research integrates cyber threats, law, and ethics into a socio-technical framework suitable for healthcare institutions. Second, an empirical gap exists because few quantitative studies have systematically examined cybersecurity in Kenyan public hospitals. Third, there is a contextual gap, since little research has been done on KNH, the largest referral hospital in East Africa, despite its size, complexity, and critical role in the national health system.

This study therefore seeks to address these gaps by examining cyber threats at KNH, analyzing the impact of the Kenya Cybercrime Act on hospital cybersecurity, evaluating the effectiveness of ethical data protection guidelines in safeguarding patient data, and proposing a socio-technical framework tailored to KNH and scalable to other healthcare providers in Kenya.

1.3 Purpose of the study

The purpose of this study was to examine the threats and countermeasures related to healthcare cybersecurity at Kenyatta National Hospital (KNH). Specifically, the study aimed to assess perceived cyber risks, analyze the role of the Kenya Cybercrime Act in supporting data protection and compliance, and examine the influence of ethical data protection guidelines in safeguarding

hospital information systems. Based on these assessments, the study sought to propose a socio-technical cybersecurity framework that integrates these dimensions to enhance resilience and strengthen cybersecurity in Kenya's public healthcare institutions.

1.4 Objectives

1) To examine the threats in healthcare cyber risk at Kenyatta National Hospital.,
2) To analyze the effects of Kenya cybercrime Act, as a local data protection laws, on supporting patient-healthcare system at Kenyatta National Hospital.,
3) To examine data protection ethical guidelines adopted by Kenyatta National Hospital to protect its healthcare system.
4) To propose framework/model for the establishment of cybersecurity measures for healthcare providers in Kenya.

1.5 Research questions

This e study was guided by the following research questions:

1. What are the measurable effects of healthcare cyber threats on the integrity and functionality of services at Kenyatta National Hospital?
2. How does the Kenya Cybercrime Act, as a local data protection law, influence patient data protection and cybersecurity compliance at Kenyatta National Hospital?
3. How effective are the data protection ethical guidelines adopted by Kenyatta National Hospital in safeguarding its healthcare system against cyber risks?
4. What framework can be developed to establish effective cybersecurity measures for healthcare providers in Kenya?

1.6 Justification of the Study

The increasing digitization of healthcare services in Kenya, particularly in public institutions such as Kenyatta National Hospital (KNH), has heightened the urgency for robust cybersecurity mechanisms to protect sensitive patient data, ensure uninterrupted service delivery, and maintain public trust. However, there is a noticeable gap in empirical research assessing the effectiveness of existing cybersecurity frameworks, staff awareness, legal compliance, and ethical data protection practices within Kenyan public healthcare institutions. This study is therefore important because it provides evidence-based insights into the specific threats, vulnerabilities, and institutional responses to cyber risks at KNH, the country's largest and most digitally advanced referral hospital.

1.7 Limitations of the Study

One limitation of this study is its reliance on self-reported data collected through structured questionnaires. While this method allows for the collection of standardized responses, it may be subject to response bias, including social desirability or inaccurate self-assessment of cybersecurity knowledge and practices. To mitigate this, the study ensured respondent anonymity and encouraged honest responses by clearly communicating that the research was for academic purposes only and that individual identities would not be disclosed.

Another limitation is the study's confinement to a single public healthcare institution, Kenyatta National Hospital., Although KNH is a national referral and teaching hospital with a complex digital infrastructure, its cybersecurity practices may not fully represent those of other hospitals across Kenya, especially at county or private levels. To address this, the study recommends future comparative research across multiple facilities to broaden generalizability. Additionally, the

study's cross-sectional design provides a snapshot in time and does not capture evolving cybersecurity trends or long-term effects of interventions, which could be addressed through longitudinal follow-up studies.

1.8 Delimitation of the Study

This study was delimited to Kenyatta National Hospital (KNH), the largest public referral and teaching hospital in Kenya. The choice of KNH was strategic due to its advanced level of digitalization and central role in national healthcare delivery, which provided a rich environment for assessing cybersecurity risks and institutional responses. By focusing on a single, high-capacity institution with established digital infrastructure, the study was able to access diverse departments, including ICT, clinical, and administrative units, ensuring a comprehensive understanding of the cybersecurity landscape within a real-world public hospital context.

The study was further delimited to three main dimensions: perceived healthcare cyber threats, the impact of the Kenya Cybercrime Act, and ethical data protection guidelines. These factors were selected because they represent the most critical elements influencing cybersecurity readiness in healthcare settings, particularly in resource-constrained public institutions. The quantitative research design and use of a structured questionnaire ensured consistency and objectivity in data collection, while stratified sampling enhanced representation across professional categories. These delimitations allowed the study to remain focused, feasible, and methodologically sound, thereby increasing the reliability and relevance of the findings.

1.9 Significance of the study

The findings of this study contribute to a broad spectrum of stakeholders within the healthcare and cybersecurity sectors. Hospital administrators and policymakers can receive empirically grounded recommendations aimed at strengthening institutional cybersecurity frameworks. Regulatory bodies, including the Ministry of Health and the Office of the Data Protection Commissioner, will gain practical insights into how national legal instruments such as the Kenya Cybercrime and Computer Misuse Act and the Data Protection Act operate within public healthcare settings. Additionally, cybersecurity professionals and health IT system developers can use the proposed framework to design contextually relevant and technically robust data protection solutions suited to the specific needs of the Kenyan healthcare environment.

Academically, the study contributes to the existing body of knowledge by applying the Socio-Technical Systems (STS) Theory to the context of public healthcare cybersecurity in a low- and middle-income country setting. It expands empirical understanding of how legal, ethical, and technical factors interact to influence cybersecurity readiness in hospitals. Furthermore, by focusing on KNH, this study provides a foundational reference for future comparative research in other public or private healthcare institutions in Kenya and the wider Sub-Saharan African region, where similar contextual and infrastructural challenges exist.

1.10 Assumptions of the Study

This study was conducted under several key assumptions that made it feasible to proceed with a reasonable degree of confidence in the integrity of its findings. First, it was assumed that the structured questionnaire used as the primary data collection instrument was both valid and reliable for capturing information on cybersecurity awareness, legal compliance, ethical practices, and

institutional preparedness. The design of the instrument was guided by existing literature and subjected to expert review to ensure content validity.

Secondly, the study assumed that the sample selected from Kenyatta National Hospital was representative of the broader population of staff involved in or affected by healthcare cybersecurity practices. Stratified sampling was used to include respondents from ICT, clinical, and administrative departments to reflect the multidisciplinary nature of cybersecurity engagement in hospital settings.

Finally, this study assumed that respondents would provide honest, unbiased, and thoughtful answers to the questionnaire items. This assumption was essential to preserving the authenticity of self-reported data. To support this, confidentiality was assured and participation was voluntary, reducing the likelihood of social desirability bias or non-cooperation. These assumptions collectively supported the internal and external validity of the study and enabled the researcher to interpret the data with justified confidence.

1.11 Operational Definition of Terms

i. **Cybersecurity** - Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks, unauthorized access, and data breaches (Ghafur et al., 2022). In this study, cybersecurity encompasses the technical, policy, and human-driven measures in place at Kenyatta National Hospital to protect patient data and digital infrastructure from cyber threats.

ii. **Healthcare Cyber Risk -** Healthcare cyber risk is defined as the potential for harm resulting from the exploitation of vulnerabilities in healthcare systems, including unauthorized access to patient records, service disruption, or manipulation of medical

devices (Obeidat et al., 2021). In this study, the term is used to describe staff perceptions of various risks affecting KNH's digital systems, including external attacks and insider threats.

iii. **Cybercrime Act (Kenya) -** The Kenya Cybercrime and Computer Misuse Act, 2018, is a legal framework that criminalizes offenses such as unauthorized system access, data interference, cyberbullying, and identity theft (Government of Kenya [GoK], 2018). In this study, it is assessed as an independent variable to evaluate its influence on institutional cybersecurity awareness and compliance at KNH.

iv. **Data Protection Ethical Guidelines -** These refer to the ethical principles and regulatory standards that guide how personal health data should be collected, stored, accessed, and shared, ensuring confidentiality, integrity, and accountability (Kenya Data Protection Act, 2019). In this study, the term is used to assess the presence and enforcement of ethical data handling practices at KNH, including staff training and policy awareness.

v. **Cybersecurity Framework -** A cybersecurity framework is a structured approach outlining how an organization identifies, prevents, detects, and responds to cyber threats (National Institute of Standards and Technology [NIST], 2018). In this study, the cybersecurity framework refers to the collective systems, policies, procedures, and controls in place at KNH to manage digital health security risks.

vi. **Perceived Threat -** Perceived threat refers to an individual's subjective judgment about the severity and likelihood of a potential cybersecurity incident (Kane & Skibinski, 2021). In this study, it reflects how KNH staff evaluate the risk of various cyber threats and how that perception influences their behavior and confidence in institutional protections.

vii. **Socio-Technical Systems (STS) Theory -** STS Theory posits that organizational effectiveness arises from the joint optimization of social (human) and technical (systemic) components (Malatji et al., 2019). In this study, STS Theory underpins the conceptual framework, guiding the analysis of how technical infrastructure, ethical policies, and human behavior interact to shape cybersecurity outcomes at KNH.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter gives a scrutiny of the available published works in light of the research study objective which was to examine the threats and counter measures in healthcare cyber risk at Kenyatta National Hospital.,

2.2 Theoretical framework

Recent cybersecurity research applies various theories depending on the context, including Resource-Based View, Social Cognitive Theory, Dynamic Capabilities, and Socio-Technical Systems Theory (Barney, 2020; Zhang et al., 2021; Liu & Huang, 2022). This study adopts Socio-Technical Systems Theory to examine how technology integrates with social and human factors in cybersecurity, emphasizing the interaction between technical systems and organizational behavior (Carroll et al., 2020; Shih et al., 2022).

2.2.1 Socio-technical system theory

STS theory emerged from organizational research in the 1950s to challenge the notion that technology alone determines system effectiveness (Trist & Bamforth, 1951). It emphasizes the interdependence between social factors (people, culture, processes) and technical components (tools, systems, infrastructure) (Pasmore et al., 1982). In cybersecurity, STS theory positions threats as socio-technical problems, where failures often arise from misalignment between technology and human or organizational elements (Malatji et al., 2019; Baxter & Sommerville, 2011).

Applying STS theory involves joint optimization balancing social and technical subsystems to avoid “socio-technical vacuums,” which create vulnerabilities exploitable by attackers (Malatji et

al., 2019). This approach necessitates integrating technological controls with user-centric measures such as awareness training, intuitive system design, and organizational policies that support secure behaviour (Bolchini et al., 2017). For example, while firewalls and encryption provide technical defenses, employee training and process improvements address the social side, reducing risks of human error.

STS theory also grounds the development of cybersecurity frameworks that incorporate maturity models and risk assessments sensitive to socio-technical dynamics (Malatji et al., 2019). This is crucial in complex organizations where cybersecurity effectiveness depends on aligning policies, culture, and technology consistently (NIST, 2017b; Friedberg et al., 2017).

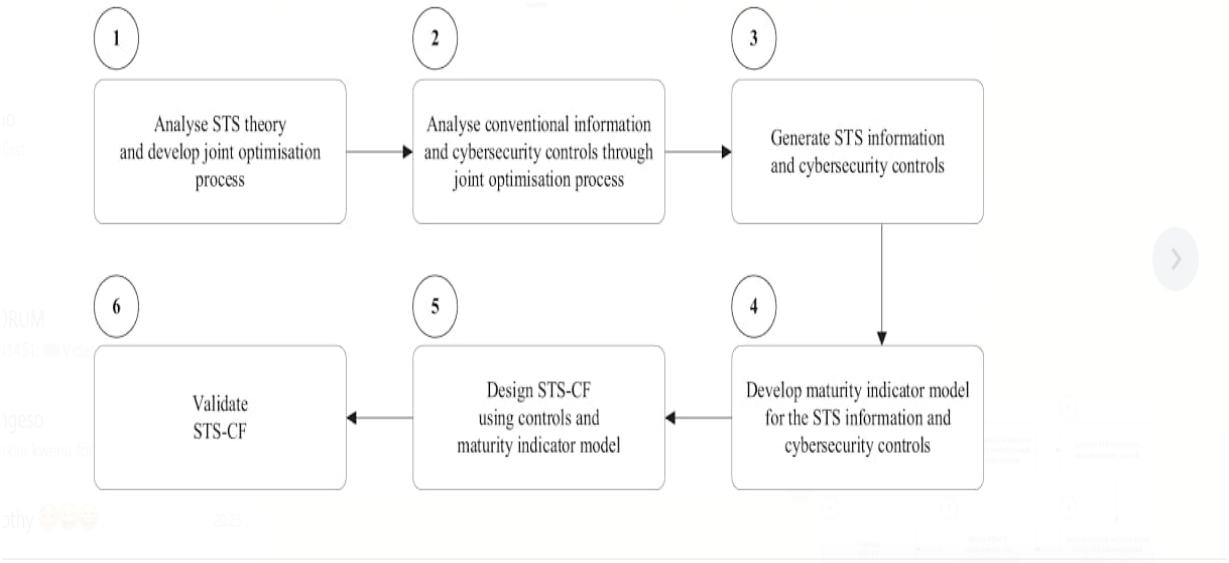
In this study, STS theory informs the investigation of how cybersecurity strategies must integrate technological tools with organizational culture and human factors to enhance resilience. By acknowledging the dynamic interaction between social and technical elements, the study aims to develop recommendations that foster comprehensive and adaptive cybersecurity practices aligned with organizational goals.

The National Institute of Standards and Technology (2017a) asserts that intricate firmware and software are included in every technological structure. Information security in systems is defined by Craigen et al. (2014) as the gathering and setting up of company resources, policies, and systems against malicious invasions. To properly secure systems and evaluate their preparedness to withstand a torrent of attacks, organizations need consistent controls in addition to a uniform architecture (NIST, 2017b). Friedberg et al. (2017) state that a careful analysis of security vulnerabilities and their possible ramifications ought to go hand in hand with the implementation of standard architecture in an organization's framework. The previous arguments make it

abundantly evident that technology systems provide far greater vulnerability issues (Wurm et al., 2017).

Figure 2.1

TS-CF development methodology



When a security solution is determined to focus too much on the social or the technological, it is thought that a socio-technical vacuum will arise. These shortcomings result in security holes that hackers can take advantage of. The collaborative optimization development approach, which is the foundation of the framework, is used to assess and categorize cybersecurity measures and available data. The joint optimization process model is verified by collaboration with two seasoned professionals (Malatji et al., 2019).

Analyze STS theory and develop joint optimization process. The socio-technical systems theory is examined, and a greater theoretical foundation with equal attention to both social and technological elements is imagined. This is referred to as the joint optimization process.

Analyze information and cybersecurity controls through the joint optimization process. The controls examined were collected from widely published and sector information and cybersecurity strategies between 2001 and 2017. This is because the frameworks will have had enough time to be evaluated and verified. An important condition is that these frameworks must precisely include components of data security, regardless of whether they are sector specific, governance, risk, or compliance oriented.

Generate STS cybersecurity controls. Security controls are developed after being assessed and subsequently submitted via the joint optimization process. Furthermore, identical controls are deleted and related ones consolidated. This leads to the development of fresh and flexible high-level STS data and cybersecurity measures.

Develop STS cybersecurity controls maturity indicator model. A suitable capability maturity model is established to assess the maturity of the deployed information and cybersecurity controls.

Develop the STS-CF. The developed safety rules and capability maturity model are integrated with the joint optimization process to construct a conceptual STS cybersecurity program.

Validate the STS-CF. Here, the validity and effectiveness of the Here, the proposed STS-CF is tested for validity and effectiveness.

2.2.2 Justification and Application of Socio-Technical Systems Theory to the Study

Socio-Technical Systems (STS) Theory is directly relevant to the purpose and objectives of this study, which sought to understand and improve cybersecurity in the healthcare context at Kenyatta National Hospital (KNH). The theory's central tenet that cybersecurity challenges arise from the complex interplay between social and technical elements aligns with the multifaceted nature of healthcare cybersecurity where technology, users, policies, and organizational culture all interact.

First objective: To examine the threats in healthcare cyber risk at KNH, STS theory provides a framework to analyze not only technological vulnerabilities but also social factors such as staff behavior, training, and organizational processes that contribute to these risks. By focusing on both sides of the socio-technical coin, the study can identify comprehensive risk areas beyond just technical flaws.

Second objective: In analyzing the impact of the Kenya Cybercrime Act on supporting patient-healthcare systems, STS theory helps to explore how legal and regulatory frameworks influence organizational policies and user practices, thereby affecting the overall cybersecurity posture. The theory's emphasis on the social subsystem encourages examination of how staff understand and comply with these laws, bridging the gap between legislation and practice.

Third objective: Regarding data protection ethical guidelines adopted by KNH, STS theory underscores the importance of aligning technical safeguards with ethical standards and staff adherence. The theory suggests that effective data protection results from embedding ethical principles within both technical controls and social behaviors, including training, awareness, and organizational culture.

Fourth objective: Finally, in proposing a cybersecurity framework/model for healthcare providers in Kenya, STS theory offers a robust foundation. The joint optimization concept guides the design of cybersecurity solutions that integrate technological defenses with human and organizational factors, ensuring that the framework is practical, adaptable, and comprehensive. This socio-technical approach increases the likelihood of successful implementation and sustainability of cybersecurity measures in complex healthcare environments.

In summary, STS theory informs the study by framing healthcare cybersecurity as a socio-technical challenge that requires coordinated technological, organizational, and human-centered strategies. This holistic perspective supports all study objectives by emphasizing that effective cybersecurity in healthcare settings must be built on the balanced optimization of social and technical systems.

2.3 General literature review

2.3.1 Threats in Healthcare Cyber Risk

The integration of digital technologies in healthcare has streamlined patient management and improved operational efficiencies. However, this digital transition has also exposed institutions like Kenyatta National Hospital (KNH) to substantial cybersecurity threats. These risks compromise sensitive patient data, disrupt critical operations, and challenge healthcare providers' ability to maintain trust and deliver quality care. This section explores the nature and impact of these threats on healthcare systems, identifies challenges faced by KNH, and highlights gaps in existing literature.

Cyber threats such as malware and ransomware pose significant risks to healthcare institutions worldwide. These attacks encrypt sensitive data and demand ransom payments, often crippling operations and delaying patient care. The WannaCry ransomware attack of 2017, which affected

healthcare systems globally, underscored the critical vulnerabilities in hospital networks (Perakslis, 2014). Healthcare institutions are prime targets because medical data is highly lucrative on the black market, with studies estimating its value to exceed that of financial data (Schmeelk et al., 2021; Choi et al., 2020). In Kenya, hospitals face compounded risks due to reliance on outdated systems and limited cybersecurity infrastructure (Zwilling et al., 2022). Despite this, few studies focus on the preparedness of Kenyan healthcare institutions, including KNH, to prevent or respond to ransomware incidents, creating a critical research gap.

Phishing and social engineering attacks are among the most persistent cybersecurity threats faced by healthcare institutions. These attacks exploit human error through deceptive emails or cloned websites, tricking staff into revealing credentials or clicking malicious links (Abdullah et al., 2020). The dynamic nature of phishing makes it especially difficult to mitigate, with research showing it as a leading entry point for cybercriminals in healthcare settings (Tolossa, 2023). In developing regions like Kenya, insufficient training on cybersecurity awareness exacerbates this vulnerability, particularly in high-pressure environments like KNH (Alahmari et al., 2014). However, there is limited empirical evidence evaluating the impact of awareness campaigns or training initiatives within Kenyan hospitals, leaving questions about their efficacy unanswered (Becerra-Fernandez & Sabherwal, 2014).

Advanced Persistent Threats (APTs) represent another growing challenge, particularly for institutions managing critical infrastructure. APTs are prolonged and targeted attacks, often orchestrated by state-sponsored actors or sophisticated cybercriminal groups, aiming to extract sensitive data or disrupt essential services (Bada et al., 2019). Research highlights the susceptibility of hospitals to such attacks due to the high value of their data and the potential for operational disruption (Kruse et al., 2017). In the Kenyan context, hospitals like KNH are

particularly vulnerable because of limited detection and response capabilities. However, existing literature largely overlooks the prevalence and impact of APTs in Kenya's healthcare sector, leaving a gap in understanding how institutions prepare for or mitigate such sophisticated threats.

Insider threats, whether due to negligence or malicious intent, further exacerbate cybersecurity challenges in healthcare. Employees or contractors with authorized access to systems may inadvertently expose sensitive data or exploit their privileges for personal gain. Studies estimate that insider threats account for up to 60% of cybersecurity incidents in healthcare (Dang-Pham & Nkhoma, 2017). This risk is heightened in resource-constrained environments like KNH, where monitoring mechanisms are often underdeveloped. While international literature discusses strategies to mitigate insider risks, there is a lack of localized research examining how Kenyan hospitals manage insider threats, particularly in contexts of limited resources and high data sensitivity (Reeves et al., 2021).

The impact of these threats on healthcare systems extends beyond financial losses to compromise patient care and public trust. Operational disruptions caused by ransomware or DDoS attacks delay treatments, disrupt diagnostics, and compromise emergency services, directly affecting patient outcomes (Choi et al., 2020). Data breaches undermine patient trust, making individuals reluctant to share critical information for fear of exposure (Elshenawy et al., 2021). Financially, cyberattacks impose heavy costs for system recovery, legal action, and compliance penalties, further straining resource-limited institutions like KNH (Schmeelk et al., 2021). Despite these documented impacts, there is limited research quantifying the specific consequences of cyber incidents on operational efficiency and patient outcomes within Kenyan hospitals, leaving a significant knowledge gap.

The implications of data breaches in healthcare are profound, exposing patients to identity theft, fraud, and compromised care. Globally, data breaches have become a leading cybersecurity

concern, with healthcare institutions accounting for a significant proportion of reported incidents (Weerasinghe et al., 2020). Studies emphasize that weak access controls and inadequate encryption are common contributors to breaches in developing countries (Elshenawy et al., 2021; Almutairi et al., 2020). At KNH, the integration of legacy systems with modern technologies creates gaps that are easily exploited by attackers. However, there is limited research exploring the systemic weaknesses specific to Kenyan hospitals, particularly in how they contribute to data breaches, highlighting a critical area for further investigation.

Despite growing recognition of cybersecurity risks in healthcare globally, there remains a significant research gap concerning the specific challenges and preparedness of institutions like Kenyatta National Hospital. Comparable studies in other low and middle income countries (LMICs) such as Nigeria and South Africa have explored the impact of resource limitations and workforce capacity on healthcare cybersecurity readiness (Akinbohun et al., 2021; Mhlongo & Moyo, 2023). These studies highlight critical issues including insufficient cybersecurity training for healthcare workers, inadequate investment in security infrastructure, and fragmented policy enforcement. However, while these findings provide valuable insights, they cannot be directly generalized to Kenya due to differences in healthcare system organization, technological adoption rates, and regulatory environments. Moreover, empirical data assessing the effectiveness of cybersecurity awareness initiatives, incident response capabilities, and integration challenges in Kenyan public hospitals remain scarce (Zwilling et al., 2022; Tolossa, 2023). This lack of localized evidence particularly regarding sophisticated threats like Advanced Persistent Threats and insider risks at KNH points to an urgent need for focused research. Addressing this gap is crucial to developing context-specific strategies that enhance the resilience of Kenyan healthcare institutions against cyber threats.

2.3.2 Kenya cybercrime Act on Healthcare Cyber Security Risks

The impact of Kenya's Cybercrime Act, 2018, on the patient-healthcare system relationship at Kenyatta National Hospital (KNH) represents a pivotal juncture where legal reform, digital security, and public health intersect. As healthcare systems adopt digitized medical records and telemedicine technologies, the protection of sensitive patient data becomes paramount. In this context, the Computer Misuse and Cybercrimes Act (CMCA) and the Data Protection Act (DPA), both central components of Kenya's cybersecurity framework, have introduced legal imperatives aimed at safeguarding information integrity, mitigating cyber threats, and ultimately reinforcing public trust in healthcare institutions. This objective calls for an examination not merely of statutory existence but of tangible influence, how these legal instruments shape the dynamics between patients and KNH, the country's largest referral and teaching hospital.

From the literature, Kenya's cybersecurity architecture, including the CMCA, is presented as a multidimensional response to emerging threats, encompassing governance, capacity building, and legislative enforcement. The Act enforces strict controls on unauthorized access and interference with data, effectively criminalizing the mishandling or leakage of sensitive patient health records. According to Ayugi (2021), this legal structure underpins the trust required for patients to disclose personal health data, an essential component in accurate diagnosis and effective treatment. The provision for data breach notification within the Act further embeds transparency and accountability into healthcare operations. In the event of a breach, healthcare institutions are legally mandated to inform affected patients, thereby reducing information asymmetry and fostering patient confidence in institutional responsiveness.

The DPA (2019), which complement the CMCA, takes a rights-based approach by explicitly codifying data subject rights, requiring informed consent, and establishing the role of data

protection officers (Nyaga et al., 2023). In clinical settings such as KNH, where thousands of patients are managed daily, these protections ensure that individuals maintain agency over their personal information. This aligns with the ethical principles where informed consent, data minimization, and transparency are underscored as critical pillars for data governance in healthcare. While the theoretical implications of these policies are robust, literature lacks empirical validation of how effectively these rights are upheld in public healthcare institutions, highlighting a significant research gap.

Additionally, literature draws on the broader impacts of cybersecurity on healthcare, emphasizing that breaches not only compromise confidentiality but also erode trust, impair diagnostic accuracy, and increase operational costs. Abdullah et al. (2020) and Weerasinghe et al. (2020) argue that in low-resource contexts, inadequate cybersecurity safeguards exacerbate these vulnerabilities. Thus, in a setting like KNH where digital health infrastructure is expanding but resources remain stretched, the presence of strong legal deterrents via the CMCA becomes a vital control mechanism. However, implementation challenges persist, including outdated IT systems and undertrained staff. Despite mandates, many institutions, especially public ones, struggle to adhere to international standards like ISO/IEC 27001 or the NIST Cybersecurity Framework raising questions about the depth of compliance at the operational level.

The literature also points to the role of compliance mechanisms and audit systems in reinforcing legal mandates. Regular internal audits, when performed effectively, identify vulnerabilities and offer prescriptive recommendations to improve cyber-readiness. Yet, literature from PricewaterhouseCoopers (2019), and Hubbard and Seiersen (2023) suggests that without proper funding and organizational buy-in, these mechanisms may remain superficial or underutilized, particularly in high-volume institutions like KNH. The KE-CIRT/CC, a national response team

established to manage and coordinate cyber incidents, provides a macro-level defense infrastructure. While its capacity for threat intelligence sharing and rapid response is critical, the extent to which it directly interfaces with or supports hospital-level security protocols remains under-explored in the reviewed literature—indicating another notable research void.

Moreover, parallels drawn from other African nations, particularly in Makulilo and Boshe (2016), show that while legislative efforts have improved data governance, their effectiveness is often undermined by institutional inertia and a lack of sector-specific regulations. Unlike the EU's General Data Protection Regulation (GDPR), Kenya's CMCA and DPA do not include healthcare-specific clauses tailored to the sensitivities of medical data. This gap may limit their contextual efficacy in hospitals, where the urgency and complexity of care delivery may challenge rigid adherence to data protection protocols.

The existing literature does recognize the CMCA's positive influence in incentivizing healthcare institutions to invest in secure digital systems and staff training. Improved technological integration at KNH, prompted by legal pressure, can facilitate safer patient data storage, enhance clinical decision-making, and reduces downtime from cyber incidents. However, the transformation is not uniformly distributed across departments. Units dealing with stigmatized conditions such as HIV/AIDS or mental health may benefit more from enhanced protections due to the heightened sensitivity of the data involved. Yet, without disaggregated institutional studies, such differential impacts remain speculative.

Further, the intersection of law and ethics in healthcare cybersecurity is critical like Ata protection guidelines rooted in ethical principles like accountability, patient empowerment, and continuous education. These are vital for embedding a culture of data stewardship. Still, ethical compliance, unlike legal compliance, is harder to measure, and often depends on institutional culture, which

varies widely within large establishments like KNH. As Omondi (2023), and Mugo and Nzuki (2014) observe, fostering a climate where staff not only understand but value ethical data handling practices is essential for the law to translate into meaningful protection for patients.

In summary, the literature affirms that Kenya's Cybercrime Act and its associated regulatory instruments provide a necessary legal scaffold for safeguarding patient data and reinforcing trust in healthcare. These frameworks establish foundational protections, promote technological advancement, and impose punitive measures against breaches. However, while the statutory intentions are clear, the literature reveals several gaps, most notably, a dearth of empirical research at the institutional level. For KNH, a flagship public hospital, there is a pressing need to assess how these laws are operationalized, whether they are adequately resourced, and how they influence patient behavior and healthcare outcomes. Comparative insights from similar legal environments underscore the potential of such laws but also caution against assuming uniform implementation or efficacy. Addressing these gaps through targeted research is crucial for understanding and enhancing the real-world impact of Kenya's cybercrime legislation on its health systems.

2.3.2.1 The Kenya Cybercrime Act and Its Role in Supporting the Patient-Healthcare System Relationship

Trust between patients and healthcare providers is fundamental to effective healthcare delivery, with data confidentiality and privacy playing a pivotal role. The Kenya Cybercrime Act of 2018, serving as a local data protection framework, has significantly influenced the relationship between patients and the healthcare system by enhancing trust and ensuring data security (Ayugi, 2021). Key Contributions of the Cybercrime Act include.

i. **Data Protection and Privacy -** The Act enforces stringent measures to safeguard patient health records and private medical information, requiring healthcare providers

to implement robust security protocols. This assurance of secure handling of sensitive data builds patient confidence in the healthcare system.

ii. **Legal Framework for Data Breach Response** - It mandates timely notification of patients in the event of a data breach, promoting transparency and accountability. This legal requirement strengthens trust by demonstrating commitment to patient privacy and security.

iii. **Encouraging Technological Advancements -** The Act drives healthcare organizations to adopt advanced cybersecurity measures, enhancing both data protection and service delivery. Improved technological integration leads to more accurate diagnoses and efficient treatment, benefiting patients directly.

iv. **Deterrence Against Cybercrime** - By imposing severe penalties for cybercrimes, including unauthorized access to medical records, the Act serves as a deterrent against data breaches. Patients gain peace of mind knowing their data is safeguarded by robust legal protections.

v. **Guidelines for International Data Transmission** - In cases requiring cross-border data sharing for specialized treatment, the Act ensures secure data transfer while aligning with international standards. This fosters patient trust in the system's capability to protect their data globally.

vi. **Promoting Trust in Healthcare Providers** - With the enhanced security measures mandated by the Act, patients are more likely to trust healthcare providers, facilitating open communication and better medical outcomes.

2.3.2.2 The Kenya Information and Communications Act (KICA) - Empowering a Digital Nation

Digital technologies have completely changed how we live, work, and communicate in the twenty-first century. Kenya, along with numerous other countries, has welcomed this digital shift, realizing its capacity to propel economic expansion, improve public services, and empower its populace. The Kenya Information and Communications Act (KICA), a legislative framework that establishes the legal and regulatory basis for Kenya's information and communications technology (ICT) industry, is essential to this digital progress. The importance of KICA, its main features, and its influence on Kenya's digital future are all examined in this essay (Wanyama, 2015). KICA was created in 1998 and then revised in 2013 in response to the evolving information and communications technology environment. Kenya required a legislative framework to protect citizens' rights and interests, manage a quickly changing industry, and promote economic growth as the digital era got underway (Amutete, 2020). KICA has the following provisions:

i. *ICT industry Regulation:* Under KICA, the Communications Authority of Kenya (CA) is designated as the regulatory agency in charge of granting licenses, supervising, and advancing the ICT industry. This clause guarantees efficient management of ICT infrastructure and services, which promotes investment, innovation, and competition.

ii. *Customer Protection*: The Act places a high priority on customer protection by mandating that service providers provide data protection, fair and transparent pricing, and high-quality services. This guarantees Kenyans have access to a dependable and safe internet environment.

iii. *Cybersecurity:* In light of the growing dangers to cybersecurity in the digital age, KICA gives the government the authority to set up procedures for safeguarding vital ICT infrastructure and combating cybercrimes, strengthening national security in cyberspace.

iv. *Digital Broadcasting:* KICA is also in charge of managing the shift from analog to digital broadcasting, making sure that spectrum resources are used effectively and increasing the availability of digital radio and television services.

v. *E-Government:* The Act encourages the use of ICT in government functions, promoting accessibility, openness, and efficiency in the provision of public services. This covers data protection, records management, and electronic signatures.

vi. *Content Regulation:* KICA deals with digital content regulation, striking a balance between the right to free speech and the necessity to guard against harmful content such as hate speech and incitement.

2.3.2.3 The Data Protection Act (DPA) in Kenya: Safeguarding Privacy in the Digital Age

Nyaga et al. (2023) claim that as our society becomes more digitally connected, the gathering and use of personal data has become essential to everything from online shopping to healthcare services. Data security and privacy problems are growing along with the amount of personal data being processed. Kenya's Data Protection Act (DPA), which was passed in 2019 to address these issues, is a critical turning point in the nation's dedication to defending the citizens' right to privacy. The main points and ramifications of the DPA in Kenya are examined in this thesis. A thorough legislative framework that governs Kenya's processing of personal data is the Data Protection Act (2019). Its main goal is to safeguard people's privacy and make sure that their personal data is handled in a way that is fair, legal, and transparent. The DPA reflects a global understanding of the significance of data privacy and is in line with the best international practices, such as the General Data Protection Regulation (GDPR) of the European Union. DPA has the following provisions.

i. *Rights of Data Subjects:* Under the DPA, people have several rights about their personal data, including the ability to access, correct, and delete it. The right to information about the processing of personal data and its intended use is granted to data subjects.

ii. *Officer for Data Protection (DPO):* A Data Protection Officer is tasked with supervising adherence to data protection regulations and is required by the Act to be appointed by specific data controllers and processors.

iii. *Consent: A key component of the DPA is consent.* Before processing a data subject's personal information, data controllers must get the subject's explicit and informed consent. The Act establishes strict requirements for consent, stressing that it must be freely provided, explicit, and easily rescinded.

iv. *Data Localization:* Under the DPA, data controllers must make sure that personal data transferred outside of Kenya is sufficiently protected. This places limitations on the cross-border movement of personal data.

v. *Data Breach Notification:* Under the Act, impacted data subjects and the Data Commissioner must be notified of any data breaches. Notifying data subjects of breaches in a timely manner is essential to reducing any potential harm to them.

vi. Data Protection Impact Assessments, or DPIAs, are mandated by law for organizations to evaluate and reduce the risks related to data processing operations that may pose a serious threat to the rights and liberties of data subjects.

vii. Kenya's Data Protection Act (2019) is a critical step in guaranteeing the protection of data security and privacy in the digital era. With data becoming more and more important in our daily lives, the DPA is a vital defense against possible misuses of personal data. Through the Act, Kenya's data protection laws are brought into compliance with international best

practices, safeguarding individual rights while promoting the development of a responsible and prosperous data economy. The DPA can assist Kenya in striking a balance between individual privacy and technological innovation, creating a more promising digital future for everybody, if it is implemented effectively and continues to raise awareness (Mukiri et al., 2021).

2.3.3 Data Protection Ethical Guidelines in Healthcare Cyber Security Risk

The implementation of data protection ethical guidelines within healthcare institutions such as Kenyatta National Hospital (KNH) reflects the critical intersection between patient rights, institutional accountability, and digital security. Ethical data protection extends beyond compliance with statutory mandates like the Kenya Data Protection Act (2019); it encompasses informed consent, confidentiality, transparency, accountability, and patient autonomy. The literature reveals that while the ethical imperative is clearly articulated in policy frameworks, empirical evidence on its institutionalization, particularly in high-volume, resource-stretched hospitals like KNH is still limited.

Globally, ethical data governance in healthcare has increasingly emphasized the role of informed consent as a foundation for patient autonomy and trust. Studies from developed health systems indicate that robust consent processes enhance both trust and treatment outcomes by empowering patients with knowledge and agency (Barcanescu, 2021; Vayena & Blasimme, 2018). In Kenya, the DPA aligns with these principles by mandating clear, informed, and revocable consent mechanisms (Nyaga et al., 2023). However, in the context of KNH, the implementation of these consent protocols has not been empirically documented. Mugo and Nzuki (2014), in a survey of EHR adoption in Kenyan hospitals, found that healthcare professionals often obtain consent as a formality, with little emphasis on patient understanding. This disconnects between ethical ideals

and clinical practice, especially in tertiary care centers, raises concerns about the depth of patient agency in data governance. Comparable studies in Uganda and South Africa report similar superficial consent practices in public hospitals, suggesting a regional implementation gap that warrants empirical exploration at KNH (Makulilo & Boshe, 2016; Dzenowagis et al., 2018).

The principle of data minimization, collecting only necessary data for specific purposes serves to mitigate the risks of unauthorized access and misuse. Although embedded in Kenya's DPA and emphasized in ethical codes Omondi (2023), evidence suggests that this guideline is inconsistently enforced. In Nigeria, Adebayo et al. (2021) found that health institutions frequently over-collect data without clear rationale, increasing exposure to breaches. Similar findings are echoed by Abdullah et al. (2020) in East Africa, where poor digitization policies lead to redundant data capture. At KNH, which interfaces with insurance databases, international research bodies, and public health agencies, the challenge is compounded by multi-stakeholder access to patient data. Yet, studies evaluating whether KNH has internal guidelines limiting over-collection, or how such guidelines are enforced across departments remain absent. This institutional gap underscores the need for research examining how ethical data minimization is operationalized in complex, multi-role public hospitals.

Confidentiality and data security are at the heart of ethical healthcare, especially in relation to sensitive medical information such as mental health, HIV status, or sexual and reproductive health. Globally, literature emphasizes that ethical data protection must include not only technical safeguards (encryption, access control) but also cultural competence and discretion in information sharing (Cohen et al., 2020; Choi et al., 2019). In Kenya, the KE-CIRT/CC and the CMCA establish national-level structures to prevent data breaches (Ouma, 2021), but institution-specific measures remain under-examined. At KNH, confidentiality breaches can have severe

consequences given its role in treating vulnerable and marginalized populations. Research by Weerasinghe et al. (2020) shows that patients who fear confidentiality breaches may withhold information, undermining clinical outcomes. Despite the critical nature of this issue, there is a dearth of published case studies assessing breach frequency, staff practices, or IT vulnerability audits at KNH. Similar evaluations from India and South Africa, such as those by Singh et al. (2018) and Mtembu et al. (2017), illustrate that where breach logs are systematically reviewed, confidentiality improves offering a comparative gap for local inquiry.

Transparency and accountability are equally emphasized as ethical pillars in healthcare data governance. Literature from the EU and Canada illustrates that clear communication about data use fosters trust and reduces resistance to digital record systems (Kluge et al., 2021; Flahault, 2019). Kenya's DPA obligates institutions to notify patients of breaches and explain data use policies, yet Omondi (2023) notes that public institutions often lack internal mechanisms to fulfill this obligation meaningfully. At KNH, there is no publicly available data on whether patients are routinely informed about how their health data is stored, shared, or potentially used for research. The absence of hospital-wide transparency metrics or routine ethics audits at KNH stands in contrast to models in Brazil and Estonia, where such audits are central to ethical compliance (de Freitas et al., 2022; Tikk & Kaska, 2020). This underscores the need for localized studies investigating whether KNH communicates its data practices clearly to patients, and how such practices vary across departments.

The right to data access, rectification, and erasure is another ethical dimension with strong international precedent. According to Vayena et al. (2018), patient access to personal records improves engagement and error correction in care processes. Kenya's DPA guarantees this right, but implementation remains fragmented. In a study of patient access in Nairobi County, Muthoni

and Waweru (2020) found that many hospitals lacked platforms for patients to review their records, with some still using paper-based systems that were inaccessible to patients. The situation at KNH remains unclear, with little literature indicating whether patient portals or complaint redress systems exist to handle data correction or deletion requests. Comparative systems in South Korea and the UK have implemented electronic dashboards for this purpose Kim and Park (2019) suggested that, KNH could benefit from similar models. The research gap here is clear: there is little to no empirical evidence on how patient data access rights are being respected or enabled at KNH.

Continuous staff training is widely regarded as essential to translating ethical data protection principles into institutional culture. Literature from Asia and North America shows that SETA (Security Education, Training, and Awareness) programs improve compliance, reduce data mishandling, and increase ethical sensitivity among staff (Reeves et al., 2021; Tolossa, 2023). Kenyan studies indicate that training is often sporadic and focuses more on clinical than digital ethics (Mugo & Nzuki, 2014). While KNH, as a teaching hospital, may have more structured training opportunities, there is no available research evaluating the content, frequency, or ethical orientation of its staff education programs. In contrast, Singapore's public hospitals implement quarterly ethics modules specifically on digital privacy with Tan et al. (2020), pointing to a possible model for KNH. This suggests a significant gap in documentation and assessment of how ethics training is institutionalized in Kenya's largest hospital.

Lastly, patient empowerment and data literacy are frequently under-emphasized in both policy and practice. Empowered patients are more likely to engage in shared decision-making and demand accountability in data handling (Mittelstadt, 2017). Studies from Tanzania and Malawi show that when patients are informed of their data rights, they ask more critical questions and identify

potential abuses (Zimba et al., 2021; Ngwira, 2018). In Kenya, however, patient education on data rights is not widely integrated into routine care. At KNH, where patient literacy levels vary, the challenge of empowering users is heightened. There is a need to examine whether patient-facing communication; verbal, written, or digital includes ethical data protection messaging. Without this, the legal guarantees of the DPA may remain inaccessible in practice.

The implications of examining this objective extend into both institutional reform and policy enhancement. First, identifying gaps in KNH's application of ethical data protection practices could inform the development of standardized protocols tailored for high-volume public hospitals. As Omondi (2023) emphasizes, ethical data governance is only effective when embedded into everyday clinical operations. A systematic evaluation of KNH's practices could therefore serve as a national benchmark for other referral facilities, particularly in contexts where digital health systems are rapidly expanding. Moreover, such an examination supports Kenya's broader digital health strategy, which aspires to integrate data protection into national e-health platforms (Ministry of Health Kenya, 2021).

At an operational level, insights from this objective may inform capacity-building priorities. For example, if gaps in staff training are identified, KNH could design modular ethics workshops modeled after global best practices (Tan et al., 2020). Similarly, if patient consent processes are found to be inadequate, hospital administrators may re-engineer intake workflows to enhance transparency. These improvements are not merely regulatory; they directly affect health outcomes, patient satisfaction, and institutional trust (Weerasinghe et al., 2020).

Nonetheless, KNH faces distinct challenges in implementing ethical data protection. As a tertiary and teaching hospital with national referral obligations, its departments are diverse, high-pressure, and resource constrained. According to Mugo & Nzuki (2014), such institutional scale often leads

to fragmented implementation of IT policies, with some departments far more compliant than others. Furthermore, reliance on donor-funded systems or third-party software common in many public institutions introduces ethical complexity around data ownership and third-party access (Makulilo & Boshe, 2016; Singh et al., 2018). The heterogeneity of digital maturity across KNH's departments further complicates the establishment of centralized, enforceable ethical standards.

Additionally, KNH's role in medical education presents both an opportunity and a risk. While it could serve as a hub for ethical data protection training, the transient nature of medical interns and students may dilute long-term accountability unless ethical instruction is deeply embedded into academic curricula (Reeves et al., 2021). Lastly, the absence of transparency reports, public disclosures of breaches, or audit summaries at KNH makes it difficult to assess whether accountability mechanisms are functioning effectively. In summary, this objective not only fills a pressing research void but also carries practical significance for institutional resilience, regulatory compliance, and patient rights. Its findings could help transform KNH from a passive implementer of ethical guidelines to an active model of data protection governance within the region.

2.3.3.1 Data Protection Ethical Guidelines in Kenyan Healthcare Systems

In Kenya's digital healthcare landscape, safeguarding sensitive patient data is vital., Ethical data protection guidelines are pivotal for ensuring the responsible handling, sharing, and security of patient information, thereby upholding privacy and fostering trust between patients and healthcare providers (Omondi, 2023).

i. **Patient Consent and Informed Decision-Making** - Healthcare practitioners must secure informed consent, ensuring patients are fully aware of how their data is collected, stored,

and used. This guideline empowers patients to retain control over their personal health information and make informed decisions about their data.

ii. **Data Minimization and Purpose Limitation** - Healthcare facilities are advised to collect only the necessary data for specified purposes, avoiding unauthorized or unrelated uses. Limiting data collection reduces the risk of breaches and unauthorized access.

iii. **Data Security and Confidentiality** - Robust data security measures must protect patient information against breaches and unauthorized access. Ensuring confidentiality builds patient trust and enhances confidence in the healthcare system.

iv. **Transparency and Accountability** - Healthcare organizations must remain transparent about their data handling practices and accountable for breaches or misuse. Openness fosters trust, while accountability ensures organizations face consequences for failing to protect patient data.

v. **Data Access and Patient Rights** - Patients have the right to access, update, or correct their health information. Facilitating this process ensures data accuracy and empowers patients to take an active role in managing their healthcare data.

vi. **Cross-Border Data Transfer** - When patient data is shared internationally, it must comply with global data protection standards, ensuring data privacy and security even beyond national borders.

vii. **Continuous Education and Training** - Regular training for healthcare professionals on ethical data protection practices keeps them updated on the latest measures, minimizing risks of data breaches and promoting ethical conduct.

viii. **Patient Empowerment and Awareness** - Educating patients about their data rights encourages informed participation in healthcare decisions and reinforces confidence that

their data is managed responsibly. Adopting these ethical guidelines strengthens data protection in Kenya's healthcare systems. By emphasizing informed consent, security, transparency, and accountability, the guidelines ensure that patient data is handled responsibly, enhancing trust and improving healthcare quality. This ethical approach ultimately contributes to better patient outcomes and well-being (Mugo & Nzuki, 2014; Makulilo & Boshe, 2016).

2.3.4 Healthcare Cyber Security Risk Framework

The establishment of a cybersecurity framework tailored for healthcare providers in Kenya is both an urgent policy necessity and a strategic institutional goal., The increasing digitization of healthcare, driven by electronic health records (EHRs), telemedicine, and health information exchanges has exposed hospitals and clinics to growing cybersecurity threats, particularly in low- and middle-income countries (LMICs) where institutional readiness remains limited (El Shenawy et al., 2021; Abdullah et al., 2020). For Kenya, where the healthcare sector is rapidly adopting digital platforms, the absence of a healthcare-specific cybersecurity framework leaves institutions vulnerable to ransomware, data breaches, and service interruptions that compromise patient safety, data integrity, and public trust.

Globally, several cybersecurity models have been implemented to guide institutional security preparedness. Among the most prominent is the NIST Cybersecurity Framework (NIST CSF), which organizes cyber preparedness into five functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). This framework has been widely adopted in the U.S. healthcare system due to its modularity and emphasis on risk-based decision-making. Likewise, ISO/IEC 27001 provides internationally recognized standards for information security management systems (ISMS), with defined control objectives, risk assessments, and compliance monitoring (Singh et

al., 2018). However, both frameworks require institutional maturity and a culture of continuous improvement that is often absent in resource-constrained settings such as Kenya's public hospitals.

In African contexts, there have been efforts to adapt these models. South Africa, for example, integrated elements of ISO standards with sector-specific protocols through the Health Information Governance and Security Framework (HIGSF), which emphasizes governance, people, process, and technology components (Mtembu et al., 2017). Nigeria has also experimented with modular, risk-based models that incorporate local threat landscapes (Adebayo et al., 2021). While Kenya has developed a National Cybersecurity Strategy and established the National KE-CIRT/CC (Ouma, 2021), these efforts remain generic and are not customized to the distinct needs of healthcare providers, where the nature of data, urgency of service, and diversity of stakeholders create unique security vulnerabilities.

The document reviewed highlights that Kenya's current cybersecurity ecosystem is defined by broad regulatory instruments such as the Computer Misuse and Cybercrimes Act (CMCA, 2018) and the Data Protection Act (DPA, 2019). These laws lay the legal foundation for information governance but fall short in offering technical guidance, especially in operationalizing security within healthcare institutions. While CMCA outlines offenses and penalties related to cybercrime, and the DPA introduces consent and data minimization principles, there is no accompanying sectoral implementation toolkit for healthcare. This legal-regulatory gap has also been observed in comparative settings such as Tanzania and Rwanda, where cybersecurity policy exists at the national level but lacks health-specific execution (Zimba et al., 2021; Kamugisha & Rugambwa, 2020).

The implications of this gap are serious. In Kenya, healthcare providers, especially public ones face low awareness of cyber hygiene, limited budgets for IT security, reliance on third-party

infrastructure, and fragmented governance structures (Munyolo, 2021; Omondi, 2023). A model suitable for Kenyan healthcare must therefore be both context-aware and resource-conscious, integrating risk assessment, policy development, technical safeguards, training, and monitoring. Notably, cybersecurity in hospitals is not just a technical concern; it is a multidisciplinary issue involving clinical workflows, patient rights, and institutional culture (Barcanescu, 2021; McLeod & Dolezel, 2018).

A core weakness in many existing frameworks is the inadequate integration of human factors—even in high-income settings. Studies show that over 80% of data breaches in healthcare stem from human error or insider threats (Zwilling et al., 2022; McCormac et al., 2017). A model for Kenya must therefore include strong emphasis on staff training, role-based access control, and organizational accountability structures. Models such as the Protection Motivation Theory Siponen et al. (2014) and Theory of Reasoned Action D'Arcy & Lowry (2019) have been used to predict staff compliance with information security policies in health settings and could inform the behavioral elements of a Kenyan framework.

Another underdeveloped area in Kenya's cybersecurity discourse is incident response and recovery planning. NIST model emphasizes the importance of the "Respond" and "Recover" functions in the NIST model. In contrast, most Kenyan healthcare facilities focus disproportionately on data protection and prevention, neglecting structured response mechanisms. Yet, response planning is essential in high-risk environments where cyberattacks could disrupt critical care, especially in emergency or ICU departments. Comparative literature from Singapore and Germany demonstrates that crisis response simulations and digital drills improve institutional agility and reduce downtime during real-world cyber events (Tan et al., 2020; Krutilla et al., 2021). No such protocols are documented for Kenyan hospitals to date.

Monitoring and continuous improvement are also critical for any cybersecurity model. Frameworks should include Key Performance Indicators (KPIs), periodic audits, and risk-scoring tools to evaluate cyber readiness. While private hospitals in Kenya may conduct these assessments internally or via external IT firms, public institutions like KNH are more likely to lack the budget or institutional impetus for self-evaluation. A model that embeds affordable audit templates, possibly aligned with the Digital Health Interoperability Framework under Kenya's eHealth Strategy, would improve sustainability (Ministry of Health Kenya, 2021).

The lack of research on localized cybersecurity frameworks for Kenyan healthcare represents a significant knowledge gap. Existing studies mostly describe legal awareness, threat typologies, or general ICT use in healthcare Mugo and Nzuki (2014) and Nyaga et al. (2023), with minimal work focused on framework development, validation, or pilot implementation. This gap not only limits policy but undermines institutional resilience and patient safety. There is also limited empirical documentation on institutional risk mapping, cost-benefit analyses of security investments, and interdepartmental security coordination in public healthcare, all of which are essential to framework design.

2.3.4.1 Elements of an Effective Cybersecurity Strategy

i. **Security Awareness -** Security awareness significantly influences information security risk, with varying levels low, medium, and high based on user habits and responsiveness to threats. For instance, Shaw et al. (2009) define cybersecurity awareness as users' understanding of security value, responsibilities, and actions to maintain safeguards. Ignorance of cyberthreats and poor technology use are major vulnerabilities exploited by hackers (Bada et al., 2019; Zwilling et al., 2022). Human error remains a predominant

cause of cyberattacks, highlighting the importance of comprehensive training programs to raise awareness (Letho, 2015). Moreover, McCormac et al. (2017) associate susceptibility to phishing with personality traits and note marginal gender differences in vulnerability.

ii. **Risk Prevention -** Risk prevention involves identifying, evaluating, and mitigating cybersecurity threats across organizational levels. Effective risk management transcends the security team, requiring a unified approach by all departments (Krutilla et al., 2021). The evolution of cyberattacks from disruptive early campaigns to sophisticated threats emphasizes the need for robust strategies (Boehm et al., 2019). Strong cybersecurity practices not only protect organizational data but also ensure the resilience of critical infrastructure and mitigate broader societal risks like identity theft and financial fraud (Hubbard & Seiersen, 2023).

iii. **Data Management -** Data management is a cornerstone of cybersecurity, ensuring data integrity, accessibility, and confidentiality amidst rising cyber risks. Yang et al. (2019) stress that robust protocols, including data classification, encryption, and access controls, are vital for safeguarding digital assets. Effective data management enables organizations to maintain operations during cyber threats, preserving stakeholder trust (Singh et al., 2018). As digital reliance grows, mastering data management is essential for mitigating risks and leveraging data's value (Youn et al., 2021).

2.3.4.2 Cyber Security Strategies

In the interconnected world of today, where information and communication technology permeate every aspect of life, cybersecurity is paramount. The rise of sophisticated cyber threats necessitates the adoption of robust cybersecurity strategies by individuals and organizations alike. This section

outlines key components of cybersecurity strategies, including risk assessment, the role of policies and procedures, employee training, and continuous monitoring.

i. **Understanding Cyber Threats** - Effective cybersecurity begins with a clear understanding of the diverse and evolving nature of cyber threats. These threats range from ransomware and phishing to malware and denial-of-service (DoS) attacks, often orchestrated by threat actors such as lone hackers or nation-states (Krebs, 2020). Vigilance and informed decision-making are essential in combating these threats.

ii. **Risk Assessment and Management** - Risk assessment and management are foundational elements of cybersecurity. Traditional risk assessment frameworks, such as the probabilistic risk assessment (PRA) model, evaluate threats based on their likelihood and potential impact (Hu et al., 2022). While these frameworks are valuable, many successful cyber-attacks emerge from poorly understood scenarios, challenging traditional approaches.

iii. **Frameworks for Risk Evaluation** - Frameworks like the OCTAVE Allegro offer structured methods for identifying and quantifying risks based on critical assets (Hashim et al., 2018). Incorporating consequences identification and prioritization allows organizations to allocate resources effectively to mitigate potential threats.

iv. **Security Policies and Procedures** - Developing and enforcing security policies and procedures are fundamental to robust cybersecurity. Research highlights the role of Protection Motivation Theory, Theory of Reasoned Action, and Cognitive Evaluation Theory in motivating employees to adhere to security protocols (Siponen et al., 2014). Employees' compliance with information security policies (ISPs) is influenced by their attitudes toward these policies, perceived vulnerability to threats, and social norms.

Integrating cognitive and affective factors into security frameworks—such as in D'Arcy and Lowry's (2019) model—provides a nuanced understanding of compliance behavior.

v. **Employee Training and Awareness** - Employees are often the first line of defense against cyber threats. Research demonstrates the significance of Security Education, Training, and Awareness (SETA) programs in fostering a cybersecurity-aware workforce (Reeves et al., 2021). Training must address evolving cyber threats, equip employees with practical skills, and promote a culture of vigilance. Key benefits of employee training include Reduction in Security Incidents: Training decreases the likelihood of breaches by increasing employee awareness of potential threats Tolossa (2023), Cybersecurity Knowledge Sharing: Encouraging knowledge sharing fosters trust and strengthens collective resilience Mermoud et al. (2018), and Remote Work Preparedness: Tailored training for remote work environments enhances organizational adaptability and security.

vi. **Continuous Monitoring and Adaptation** - Given the dynamic nature of cyber threats, organizations must adopt a strategy of continuous monitoring and adaptation. Real-time threat detection and analysis enable proactive identification and mitigation of vulnerabilities before they are exploited (National Cybersecurity Center of Excellence [NCCoE], 2018). Advanced monitoring systems analyze network traffic, system activity, and user behavior to detect malicious activity (Srinivasan et al., 2019). This proactive approach minimizes the potential impact of cyberattacks, safeguarding sensitive data and organizational reputation. Key Features of Continuous Monitoring include Risk Tolerance Alignment: Ensures that security measures are consistent with organizational goals, Threat Neutralization: Identifies and addresses vulnerabilities promptly to prevent exploitation

(Deshmukh-Bhosale & Sonavane, 2019) and Regulatory Compliance: Reduces the risk of legal and reputational harm due to cybersecurity lapses.

By integrating these strategies risk assessment, robust policies, employee training, and continuous monitoring organizations can effectively combat the complex and ever-evolving landscape of cyber threats. The importance of a proactive and adaptive approach cannot be overstated in ensuring cybersecurity resilience.

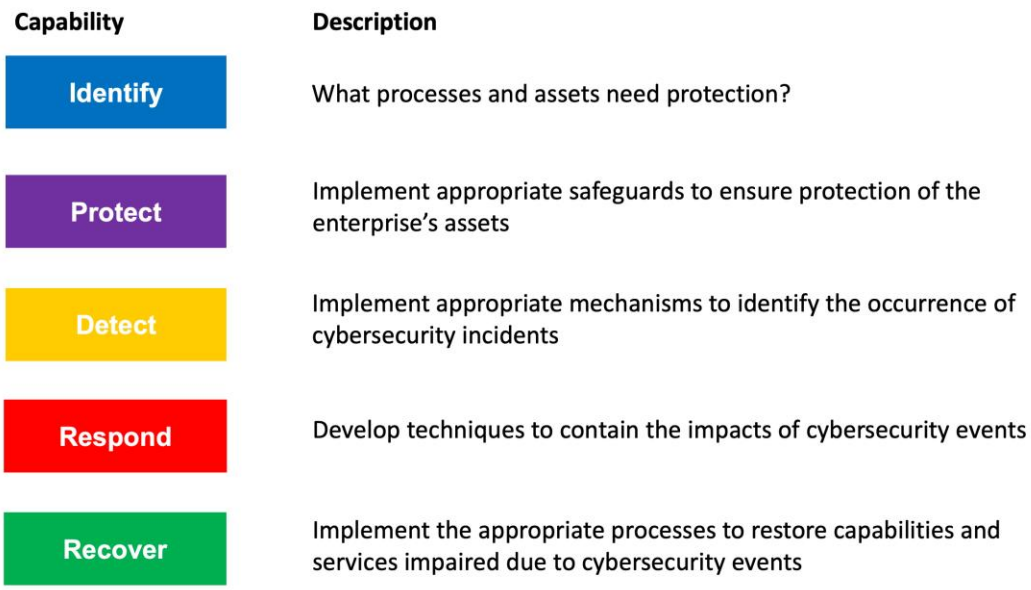
2.3.4.3 NIST cyber security framework

The NIST cybersecurity framework is a helpful tool for planning and improving your cybersecurity program. It is a set of guidelines and suggested practices meant to assist companies in enhancing and fortifying their cybersecurity posture. The framework offers a set of recommendations and guidelines that assist businesses in recognizing and detecting cyberattacks, in addition to instructions on how to respond to, prevent, and recover from cyber-disasters.

The National Institute of Standards and Technology (NIST) created this framework to address the dearth of cybersecurity standards and provide businesses with an industry-wide set of uniform norms, guidelines, and standards. Most people agree that the NIST Cybersecurity Framework (NIST CSF) is the best model for developing a cybersecurity strategy. The framework can be helpful whether you're just getting started with building a cybersecurity program or have a very established one already, as it functions as a top-level security management tool for evaluating cybersecurity risk across the organization.

Figure 2.2

NIST Cybersecurity Framework



The framework divides all cybersecurity talents, initiatives, workflows, and regular tasks into these five fundamental functions as shown above.

i. **Identify** - The Identify function establishes a foundation for cybersecurity by defining risks to systems, people, assets, and data. It involves asset identification, understanding business context, defining governance policies, assessing risks, and developing risk and supply chain management strategies tailored to organizational needs.

ii. **Protect** - The Protect function implements safeguards to minimize the impact of cybersecurity incidents. Key actions include identity management, access controls, data security measures, security awareness training, and maintenance protocols to ensure system security and resilience.

iii. **Detect** - This function emphasizes identifying cybersecurity events promptly through anomaly detection, continuous monitoring, and evaluating the effectiveness of preventive actions.

iv. **Respond** - The Respond function focuses on mitigating the impact of detected incidents. Key activities include coordinating information flow, following response plans, investigating incidents, implementing mitigation measures, and leveraging lessons learned to improve future responses.

v. **Recover** - The Recover function ensures resilience and restores compromised services following an incident. It involves recovery planning, implementing improvements based on lessons learned, and coordinating communications to return to normal operations efficiently.

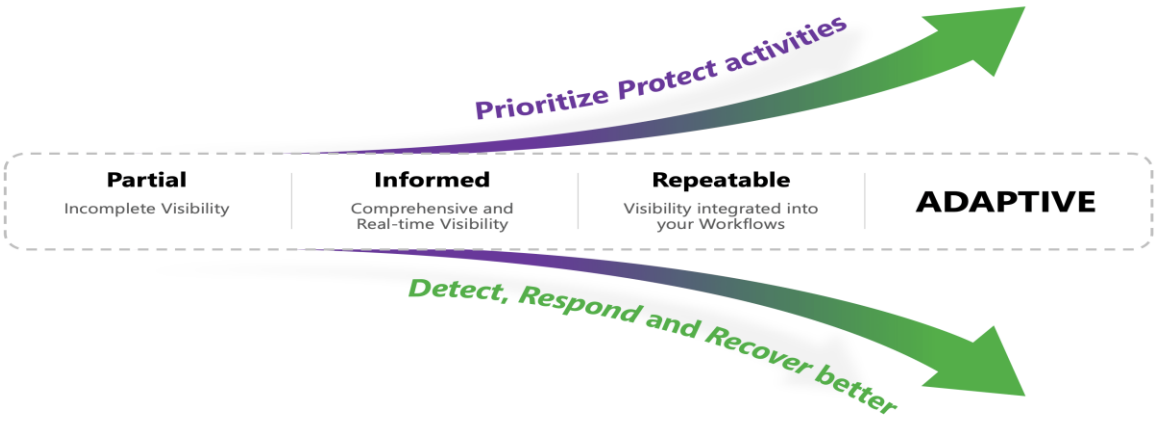
2.3.4.4 Putting your cyber security program into action and making it better

The Identify function is the most important NIST CSF function, even if each function is important for a different reason. Determining the criticality of IT assets and correctly identifying them are the fundamental ideas of Identify. Determine vulnerabilities that potential attackers may exploit as a point of entry. Your senses are comparable to your identifying abilities, which guide your cybersecurity program.

In establishing the foundational structure of a cybersecurity program, it is advisable to begin with the Identify function. This function serves as the basis upon which the other core cybersecurity functions are structured. The diagram below illustrates the interrelationship between the Identify function and the subsequent components of a comprehensive cybersecurity framework.

Figure 2.3

The Identify Function is Foundational



2.3.4.4 Current Cybersecurity Countermeasures in Kenya

National KE-CIRT/CC - The National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) plays a vital role in Kenya's cybersecurity infrastructure by managing, monitoring, and responding to cybersecurity incidents. Established under the Kenya Information and Communications Act of 1998 and operational since 2017, the center enhances Kenya's cyber-resilience through threat intelligence, incident response, and public awareness initiatives (Ouma, 2021; Bada et al., 2014). Key responsibilities include.

- **Incident Response**: KE-CIRT/CC evaluates and responds to cybersecurity incidents, including malware outbreaks, data breaches, and denial-of-service attacks.

- **Threat Intelligence**: It gathers and analyzes cyber threat intelligence, proactively sharing findings to mitigate attacks.
- **Coordination**: Facilitates collaboration among government agencies, law enforcement, ISPs, and private companies to address cybersecurity issues effectively.
- **Capacity Building**: Offers training, workshops, and seminars to strengthen the cybersecurity skills of professionals across sectors.
- **Guidelines & Best Practices**: Develops and distributes standards on risk management, secure practices, and incident response planning to bolster organizational cybersecurity.
- **Public Awareness**: Promotes safe online behavior and educates the public about cyber threats through awareness campaigns, reducing vulnerability to cybercrimes.

The National KE-CIRT/CC underscores Kenya's commitment to enhancing its digital safety through coordinated, proactive, and comprehensive cybersecurity measures.

2.4 Conceptual framework

This section outlines the key variables that form the basis of the study's conceptual framework. It identifies the primary factors influencing cybersecurity readiness at Kenyatta National Hospital, categorizing them into independent and dependent variables to clarify their relationships and guide the research focus.

Independent Variables

1. **Cybersecurity Threats -** These include a variety of risks such as malware, ransomware, phishing attacks, insider threats, and Advanced Persistent Threats (APTs) that directly challenge the security of healthcare systems.

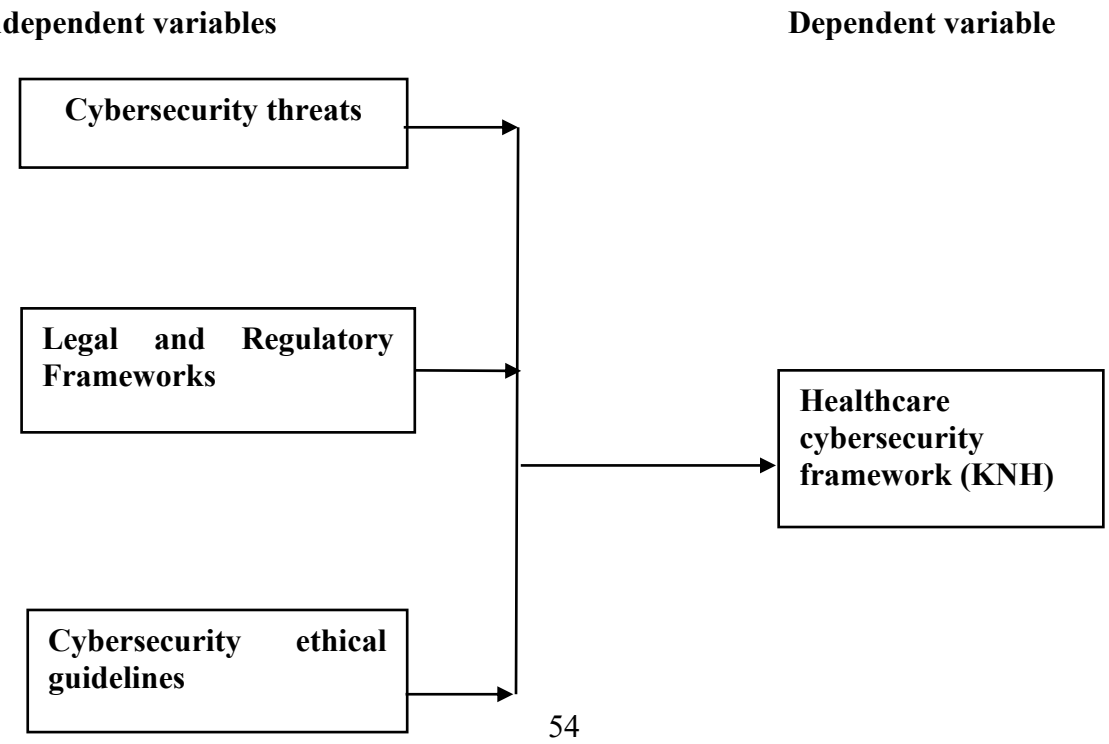
2. **Legal and Regulatory Frameworks -** This variable encompasses the national cybersecurity and data protection laws, including the Kenya Cybercrime and Computer Misuse Act and the Data Protection Act, which set the standards and obligations for securing healthcare data.
3. **Ethical and Organizational Safeguards -** This involves the policies, ethical guidelines, staff training, and technical measures adopted by the hospital to protect patient data and maintain secure healthcare operations.

Dependent Variable

1. **Healthcare cybersecurity framework -** This reflects Kenyatta National Hospital's overall ability to prevent, detect, respond to, and recover from cybersecurity incidents while ensuring compliance, operational continuity, and safeguarding patient information.

Figure 4.4

Conceptual framework



CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the methodology adopted for the study, including the research design, study location, population, sampling procedures, data collection instruments, analysis techniques, and ethical considerations.

3.2 Research Design.

The study adopted a descriptive research design to investigate cybersecurity threats and countermeasures at Kenyatta National Hospital (KNH). A descriptive design was appropriate because it enabled the systematic collection of data on staff perceptions and institutional practices without manipulating variables, while also allowing the use of both descriptive and inferential statistics to establish relationships between constructs (Creswell & Creswell, 2018; Saunders et al., 2019).

3.3 Research approach

A quantitative research approach was employed. This approach was suitable because the study sought to measure predefined variables; cybersecurity threats, the Kenya Cybercrime Act, ethical data protection guidelines, and the hospital's cybersecurity framework and test their relationships statistically. Structured questionnaires with Likert-scale items were used to generate numerical data for analysis through correlation, regression, and ANOVA, ensuring objectivity and replicability of findings (Fetters et al., 2020; Saunders et al., 2019).

3.4 Population and sampling design

This section outlines the target population for the study and the sampling design used to select a representative subset of respondents. It describes the criteria for defining the population, the

rationale for choosing specific sampling techniques, and how the sample size was determined to ensure reliable and valid results. Proper population identification and sampling are critical to generalizing the study findings accurately.

3.4.1 Population

The target population for this study comprised all employees of Kenyatta National Hospital (KNH), the largest referral and teaching hospital in Kenya. Given the study's focus on cybersecurity, the relevant groups were clinical staff, ICT personnel, and health records and administrative staff, as they are directly involved in patient care, information management, and IT infrastructure. These categories were considered integral to understanding cybersecurity threats and countermeasures in the hospital. The accessible population included staff members who were available and willing to participate during the data collection period (Creswell & Creswell, 2018; Saunders et al., 2019).

Table 3.1

Total Approximate Staff at Kenyatta National Hospital

Category	Department/Unit	Examples of Staff	Estimated Staff Count
Clinical Staff	Medical, Surgical, ICU, Pediatrics	Doctors, Nurses, Clinical Officers	4,100
Technical/IT Staff	ICT Department	Systems Administrators, IT Officers, Cybersecurity Analysts	231
Health Records & Admin	Records, HR, Finance	Records Officers, HR Managers, Accountants	602
Support Services	Maintenance, Security, Catering	Technicians, Security Officers, Cleaners	750
Academic/Training	KNH-UoN Collaborative Units	Trainers, Research Assistants, Clinical Educators	200
Management & Executive	Hospital Administration	Directors, Deputy Directors, Departmental Heads	100
Total Estimated Staff			**5,983**

3.4.2 Sampling technique and sample size

In research, sampling plays a vital role in ensuring that findings are valid, reliable, and generalizable to the broader population. As noted by Singh and Masuku (2014), sampling involves identifying and selecting a portion of a larger group in a manner that allows the results obtained from the sample to be extended to the entire population. For this study, the sample needed to adequately represent the diverse professional categories at Kenyatta National Hospital (KNH).

Given the heterogeneous nature of the hospital workforce, comprising medical personnel, clinical officers, administrative staff, and technical support, a stratified random sampling technique was deemed the most appropriate. This method increases representativeness by ensuring all key subgroups (strata) are proportionally included in the sample. Stratified sampling involves dividing the population into distinct, non-overlapping strata based on shared characteristics such as job roles or departments. Within each stratum, simple random sampling was used to select participants. This approach ensured that there was high homogeneity within each stratum and significant variation between strata, thus improving the accuracy and reliability of the data collected.

The sample size of 370 was determined based on a population of 4,933 staff members relevant to the study (clinical staffs, ICT, and health records and admin staffs) out of an approximate total population of 5983(total staffs at KNH), using a 95% confidence level and a 5% margin of error, following the Yamane (1968) sample size formula. The sample was proportionally allocated across the various staff categories to maintain statistical integrity.

$n = N/\ 1+N(e2)$

Whereby; -

n = sample size

N = Total population

1 = constant

e^2=estimated standard error equal to 5% for confidence level of 95%.

$$n = \frac{4933}{1 + 4933(0.5)2}$$

n=370

Table 3.2

Sample size table

Category	Department/Unit	Examples of Staff	Estimated Staff Count	Sample size
Clinical Staff	Medical, Surgical, ICU, Pediatrics	Doctors, Nurses, Clinical Officers	4,100	307
Technical/IT Staff	ICT Department	Systems Administrators, IT Officers, Cybersecurity Analysts	231	17
Health Records & Admin	Records, HR, Finance	Records Officers, HR Managers, Accountants	602	45
			4933	**370**

3.5 Data collection Instruments

This section outlines the research instruments employed for data collection, detailing their design, development, and the allocation based on respondent categories. The primary instrument used was a structured questionnaire developed specifically for this study, tailored to capture relevant data from relevant groups of respondents for this study, such as clinical staff, technical/IT staff, and Health records and admin staff. The questionnaire comprised sections aligned with the study's objectives, featuring Likert-scale items, multiple-choice questions, and open-ended responses where appropriate. The number of questionnaires distributed corresponded to the sample size

determined for each respondent category, ensuring proportional representation and comprehensive data collection across all relevant staff groups. The questionnaire items were structured using a five-point Likert scale to quantify the degree of agreement, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). This scale facilitated the quantification of attitudes and perceptions for statistical analysis. To examine the relationships between the independent and dependent variables, correlation analysis was employed, enabling assessment of the strength and direction of associations. The five-point Likert scale used in this study is as follows:

- Strongly Agree (SA) – 5 points
- Agree (A) – 4 points.
- Neutral (N) – 3 points.
- Disagree (D) – 2 points.
- Strongly Disagree (SD) – 1 point

Prior to deployment, the instruments underwent a pilot test to refine clarity, relevance, and reliability.

3.5.1 Pilot study

A pilot study was conducted at Mbagathi Hospital to pretest the research instruments, ensuring that the questionnaire items effectively capture the intended information and identifying any ambiguities or inconsistencies. Conducting a pilot test is critical for validating the clarity, relevance, and reliability of the data collection tools before the full-scale study (Huang et al., 2020; van & Hundley, 2021). Recent methodological literature recommends that a pilot study should involve between 10% to 20% of the total sample size to provide sufficient data for evaluating instrument performance (Connelly, 2020; Johanson & Brooks, 2010). Accordingly, this research

adopted a 20% pretest proportion, selecting participants from a population similar to the main study but external to the actual sample frame.

The pilot study helped identify unclear questions, assess the flow and timing of the questionnaire, and evaluate the reliability of the scales used. Feedback from the pilot participants led to revisions that improved question wording, eliminated redundant items, and enhanced overall instrument validity. Reliability testing using Cronbach's alpha during the pilot phase ensured internal consistency of the questionnaire constructs, aligning with best practices in survey research (Tavakol & Dennick, 2011). By addressing potential weaknesses during the pilot, this study enhanced the rigor and credibility of its data collection instruments, thereby improving the quality of subsequent data analysis and findings.

3.5.2 Validity

Validity refers to the extent to which a research instrument accurately measures the intended variables and produces trustworthy findings (Taherdoost, 2016). In this study, validity was enhanced through a pilot test used to refine the questionnaire, consistent administration of the tool across respondents, and stratified sampling to ensure that the sample represented KNH's diverse workforce. These measures increased both the accuracy of results and the generalizability of the findings to similar healthcare institutions (Heale & Twycross, 2015).

3.5.3 Reliability

Reliability refers to the consistency of a research instrument in producing stable results across repeated applications (Drost, 2018). In this study, reliability was enhanced through standardized administration procedures and a pilot test to refine the questionnaire. Internal consistency was assessed using Cronbach's alpha, which yielded a coefficient of 0.691 across the four items as

shown in Table 3.3. While slightly below the ideal 0.7 threshold, this value is acceptable in exploratory research, indicating that the instrument had adequate reliability for the study.

Table 3.3

Reliability test

Reliability Statistics	
Cronbach's Alpha	N of Items
.691	4

3.6 Methods of Data Collection

This study employed a structured questionnaire as the primary data collection instrument to gather quantitative data from the selected respondents. The questionnaire was designed to align with the study's objectives and was distributed to participants across different staff categories at Kenyatta National Hospital., To ensure the collection of accurate and reliable data, the researcher followed a systematic approach that included careful planning, obtaining necessary approvals, and applying ethical considerations.

3.6.1 Data Collection Procedures

Before data collection commenced, formal authorization was sought from the Kenyatta National Hospital administration and relevant ethics review boards. Permission letters and research clearance certificates were obtained to comply with institutional regulations and to gain access to the hospital premises and staff. These approvals facilitated cooperation from hospital management and fostered trust among respondents.

The questionnaires were administered in person by the researcher and trained research assistants who provided clear instructions on how to complete the instrument. This face-to-face approach allowed for clarification of any ambiguities and helped ensure respondents fully understood the

questions, thereby enhancing data quality. To reach respondents across different shifts and departments, data collection was scheduled flexibly, accommodating the hospital's busy operational environment.

3.6.2 Ensuring High Response Rates

Several strategies were employed to maximize response rates. First, the researcher established rapport with participants by explaining the purpose and significance of the study, emphasizing confidentiality and the voluntary nature of participation. Second, follow-up reminders were given to participants who had not returned completed questionnaires within the agreed timeframe. Third, the researcher ensured the questionnaires were concise and user-friendly to minimize respondent fatigue. Additionally, data collection was conducted within a defined, reasonable period to maintain participant engagement and reduce attrition.

3.6.3 Ethical Considerations

i. **Ethics and Approval -** The respondents were briefed on the purpose of the research in order to prevent selective perception, which is the inherent tendency to identify and quickly forget events or situations that trigger some discomfort either emotionally, physically or mentally which also are contrary to individual's strongly held beliefs. Similarly, briefing was done to curtail selective exposure, which is the behavior that would cause the respondent to favor only information that is in consonance with held beliefs and aspirations. Emphasis was placed on not causing any harm or fear whatsoever to the respondents. Approval from the department of library science of the Kenya Methodist University as well as the National Commission for Science Technology and Innovation (NACOSTI) which is mandated with the responsibility of protecting human subjects in research was sought.

ii. **Consent form -** According to Miller and Bell (2002), informed consent defines the right of the participants to understand what they are being involved in, and to voluntarily agree to participate or not to participate. All respondents who voluntarily agreed to participate were informed of the reason for conducting this research before being given the questionnaire to fill. Additionally, they were clearly informed that there was no incentive for participating in the study. This form was clearly labeled and marked with the Kenya Methodist University logo at the top of the form. All participants read, understood and signed the consent form which was provided before beginning the exercise.

iii. **Debrief form -** All participants were debriefed about the purposes for the research and the benefits accruing thereof. The debrief form contained information regarding confidentiality and the anonymity of the participants.

iv. **Anonymity and Confidentiality -** All the information that was collected from the participants was treated with the utmost confidentiality in order to avoid any psychological or physical harm.

v. **Storage and Disposal of Research Information -** The researcher took great care to protect all exercise-related materials, both digitally scanned and tangible, including the consent forms. The data was gathered from the respondents by research assistants, and it was safely kept in the university library repository

3.7 Operational Definition of Variables

For this study, abstract concepts were translated into measurable indicators to enable statistical analysis. Each variable was operationalized as follows:

- **Cybersecurity Threats (Independent Variable):** Measured by the frequency and severity of incidents such as malware, phishing, and data breaches, based on staff perceptions rated on a Likert scale.
- **Effect of the Kenya Cybercrime Act (Independent Variable):** Assessed through respondents' views on the Act's effectiveness in safeguarding health data, compliance, and enforcement within KNH.
- **Data Protection Ethical Guidelines (Independent Variable):** Defined by staff awareness, adherence to confidentiality and privacy standards, and reported compliance with hospital policies.
- **Cybersecurity Framework (Dependent Variable):** Captured by indicators of institutional preparedness, including presence of protocols, staff training programs, and adoption of technical controls.

These operational definitions guided the design of the structured questionnaire and ensured that each construct was measured systematically and aligned with the research objectives.

3.8 Data Analysis

Quantitative data were cleaned, coded, and analysed using SPSS version 21. Descriptive statistics (frequencies, percentages, means, and standard deviations) summarized respondent demographics and the key study variables. To address the research objectives, correlation, multiple regression, and ANOVA were applied to examine the joint effect of the independent variables' cybersecurity threats, the Kenya Cybercrime Act, and data protection ethical guidelines on the dependent variable, the hospital's cybersecurity framework.

The analysis process included:

- **Descriptive statistics** to establish the prevalence and patterns of cybersecurity threats.
- **Correlation analysis** to test the associations among the study variables.
- **Multiple regression and ANOVA** to evaluate the combined predictive influence of the independent variables on the cybersecurity framework.

These analyses generated empirical evidence that informed the development of a cybersecurity framework tailored for healthcare institutions in Kenya.

3.9 Chapter summary

This chapter outlined the methodology of the study, which adopted a descriptive design and quantitative approach to examine cybersecurity threats and countermeasures at Kenyatta National Hospital. The target population comprised clinical, ICT, and health records staff, with a representative sample selected through stratified sampling. Data were collected using structured questionnaires, tested for validity through a pilot study, and for reliability using Cronbach's alpha. Variables were operationalized into measurable indicators, and data were analyzed in SPSS using descriptive statistics, correlation, regression, and ANOVA to assess the joint effect of the independent variables on the hospital's cybersecurity framework, all under strict ethical considerations.

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETETION

4.1 Introduction

This chapter presents the analysis of data collected to address the study objectives. It examines the nature of cyber threats at Kenyatta National Hospital, the impact of the Kenya Cybercrime Act, the ethical data protection guidelines in place, and the frameworks that can enhance cybersecurity in healthcare institutions in Kenya

4.2 Demography

4.2.1 Response Rate

The research issued a total of 370 questionnaires out of which 365 were filled and returned giving a response rate of 94.8%. According to Mugenda and Mugenda (2002) a sample size of 30% and above was considered sufficient for the study, hence the 94.8% response rate was considered sufficient as presented in table 4.1.

Figure 4.1

Response Rate

Variable	Frequency	Percentage %
Filled and returned	365	98.65
Non-response	5	1.35
Total	**370**	**100**

4.2.2 Respondents Age

The analysis of the respondents' age distribution reveals a diverse range of age groups participating in the study as shown in Table 4.2. The age category with the highest representation is the 41-50 years group, which comprises 110 respondents, accounting for 30% of the total sample. This is followed by the 51-60-year-old age group, with 90 respondents making up 25% of the sample. The

31-40-year-old age group is also significantly represented, with 85 respondents, constituting 23% of the total. The youngest age category, 21-30 years, includes 35 respondents, representing 10% of the sample. Lastly, the age group of 61 years and older comprises 45 respondents, making up 12% of the overall sample. In total, the study surveyed 365 respondents, with the age distribution highlighting a substantial representation of middle-aged individuals.

Figure 4.2

Respondents' Age

Variable	Frequency	Percentage
21-30	35	10
31-40	85	23
41-50	110	30
51-60	90	25
61+	45	12
Total	365	100

4.2.3 Respondents Gender

The gender distribution of the respondents is depicted in Table 4.3. Majority of the respondents are male, with 210 individuals accounting for 58% of the total sample. Female respondents make up the remaining 42%, with 155 individuals. This gender distribution provides valuable insights into the study's subject matter, highlighting potential gender-related perspectives and differences within the sample population.

Figure 4.3

Respondents Gender

Variable	Frequency	Percentage
Male	210	58
Female	155	42
Total	**365**	**100**

4.2.4 Education

As shown in Table 4.4, most respondents (47%) had a bachelor's degree, followed by 24% with vocational training and 21% with a master's degree. Smaller proportions had secondary education (6%) or a PhD (3%). This distribution indicates that the sample was largely composed of well-educated staff, with a balance of both academic and technical training backgrounds relevant to the study context.

Figure 4.4

Level of Education

Variable	Frequency	Percentage
Secondary Education	20	6
Vocational training Institution	85	24
Bachelor's Degree	170	47
Msc	75	21
Phd	15	3
Total	365	100

4.2.5 Position

Table 4.5 shows that nurses formed the largest group of respondents, 120 (33%), followed by doctors, 65 (18%), and administrative staff, 60 (17%). Auxiliary personnel accounted for 50 (13%), while laboratory staff were 35 (10%) and technical staff 25 (7%). A smaller group of 10

(3%) fell under the “Other” category. This distribution reflects the diverse professional roles at KNH, with nurses and doctors forming the core of clinical staff, supported by administrative, laboratory, technical, and auxiliary functions.

Figure 4.5

Position Held

Variable	Frequency	Percentage
Doctor	65	18
Nurse	120	33
Auxiliary personnel	50	13
Lab. personnel	35	10
Administrative personnel	60	17
Technical personnel	25	7
Other	10	3
Total	**365**	**100**

4.3 To examine the threats in healthcare cyber risk at Kenyatta National Hospital.

The first objective aims to identify and assess the different types of cybersecurity threats affecting healthcare systems at Kenyatta National Hospital, highlighting the challenges these risks pose to data security and patient safety.

Figure 4.6

Descriptive analysis on Threats in Healthcare Cyber Risk at KNH

Items	N	Mean	Std Dev.	Var
KNH is vulnerable to external cyberattacks such as ransomware, phishing, and DDoS.	365	4.18	1.091	1.191
Insider threats include unauthorized access, data leaks, and staff negligence	365	3.92	1.185	1.405
Medical devices and systems face risks from outdated software, insecure devices, and weak encryption.	365	3.99	1.125	1.266

Cyber risks disrupt hospital operations through outages, record loss, and communication breakdowns	365	3.88	1.228	1.509
KNH lacks sufficient risk assessment, monitoring, and incident response planning.	365	4.04	1.157	1.339
Total Avg	**365**	**4.00**	**1.16**	**1.34**

Table 4.6 presents respondents' perceptions of healthcare cyber risks at KNH. The overall mean score was 4.00 (SD = 1.16, Var = 1.34), indicating general agreement on the existence and significance of such risks. External cyberattacks, including ransomware and phishing, ranked highest with a mean of 4.18 (SD = 1.09, Var = 1.19), reflecting strong consensus that these are the most critical threats. Deficiencies in risk assessment and monitoring followed at 4.04 (SD = 1.16, Var = 1.34), suggesting broad recognition of gaps in proactive measures.

Concerns about vulnerabilities in medical devices and systems scored a mean of 3.99 (SD = 1.13, Var = 1.27), while insider threats such as unauthorized access and data leaks averaged 3.92 (SD = 1.19, Var = 1.41). Risks of operational disruption due to system outages or record inaccessibility were rated lowest at 3.88 (SD = 1.23, Var = 1.51), though still considered significant.

Overall, the results indicate that respondents perceive cyber risks at KNH as multifaceted, with external threats and inadequate monitoring being the most pressing concerns.

4.4 To analyze the Effect of the Kenya Cybercrime Act on supporting patient-healthcare systems at KNH.

The second objective analyzed the impact of the Kenya Cybercrime Act on supporting patient-healthcare systems at Kenyatta National Hospital, assessing its effectiveness in mitigating cyber risks within the healthcare environment.

Figure 4.7

Descriptive analysis of Effect of the Kenya Cybercrime Act on supporting patient-healthcare systems at KNH.

Items	N	Mean	Std Dev	Var
The Kenya Cybercrime Act has strengthened the legal protection of patient health data at KNH by criminalizing offenses like unauthorized access, data breaches, and system interference.	365	3.95	1.134	1.286
KNH staff are sufficiently aware of the Kenya Cybercrime Act provisions, such as those concerning lawful data access, storage, sharing, and penalties for misuse of patient information.	365	4.05	1.104	1.220
Enforcement of the Kenya Cybercrime Act has helped reduce cyber incidents at KNH, such as hacking attempts, internal data misuse, or email-based phishing frauds	365	3.95	1.039	1.079
KNH has integrated the Kenya Cybercrime Act into its policies and systems, including rules on access control, audit trails for user activity, and IT security protocols in line with legal requirements.	365	3.97	1.100	1.211
The Kenya Cybercrime Act contributes to building patient trust, by ensuring their medical records are handled securely and protected from unlawful access or digital fraud.	365	4.06	1.123	1.260
Total Avg	**365**	**3.99**	**1.10**	**1.21**

Table 4.7 presents respondents' views on the impact of the Kenya Cybercrime Act at KNH. The overall mean was 3.99 (SD = 1.10, Var = 1.21), indicating broad agreement on its positive contributions, though with moderate variability. The highest-rated item was that the Act enhances patient trust, 4.06 (SD = 1.12, Var = 1.26), followed closely by staff awareness of its provisions, 4.05 (SD = 1.10, Var = 1.22). Legal protection of patient data and reduction of cyber incidents

each scored 3.95, while integration of the Act into KNH policies was rated at 3.97. Overall, the findings suggest that the Cybercrime Act is perceived to strengthen legal protections, increase awareness, support enforcement, and improve patient confidence in healthcare data security at KNH.

4.5 Examine data protection ethical guidelines on Healthcare Cybersecurity risks at KNH.

The third objective examined the data protection ethical guidelines implemented at Kenyatta National Hospital and their role in mitigating healthcare cybersecurity risks.

Table 4.8 summarizes respondents' views on ethical practices in patient data management at KNH. The overall mean was 3.94 (SD = 1.17, Var = 1.38), showing general agreement that ethical standards are upheld, though with moderate variability in perceptions. The highest-rated item was the implementation of confidentiality, integrity, and availability principles, 4.01 (SD = 1.19, Var = 1.42). Staff training on ethical standards scored 3.98, accountability for ethical violations 3.97, and patient communication 3.93, while the presence of a documented code of ethics scored slightly lower at 3.83.

Overall, the findings indicate that KNH maintains key ethical practices through policies, training, enforcement, and communication, though differences in perceptions point to opportunities for strengthening consistency across departments.

Figure 4.8

Descriptive analysis on Influence of Data Protection Ethical Guidelines on Healthcare Cybersecurity risks at KNH

	N	Mean	Std Dev	Var
KNH has a documented code of ethics that defines how patient data should be accessed, stored, shared, and protected to ensure responsible use.	365	3.83	1.166	1.359
KNH provides regular training to staff on ethical standards for handling patient information, including issues like confidentiality, informed consent, and professional conduct.	365	3.98	1.182	1.398
KNH implements the principles of confidentiality, integrity, and availability by using secure login systems, restricted access to sensitive files, and reliable data backup procedures.	365	4.01	1.193	1.423
KNH takes disciplinary action when ethical violations occur, such as unauthorized access to medical records, negligent disclosure of private data, or mishandling of patient files.	365	3.97	1.176	1.384
Patients at KNH are informed about how their personal health data is handled, including who can access it, the purposes for data use, and their rights under ethical and legal guidelines.	365	3.93	1.152	1.328
Total Avg	**365**	**3.94**	**1.17**	**1.38**

4.6 To propose a framework for the establishment of cybersecurity measures in healthcare at KNH.

The fourth objective focused on proposing a comprehensive framework or model to establish effective cybersecurity measures within the healthcare system at Kenyatta National Hospital. Table 4.9 presents respondents' perceptions of the cybersecurity framework at KNH. The overall

mean was 2.90 (SD = 1.44, Var = 2.07), indicating generally low to moderate agreement on the adequacy of current measures, with high variability reflecting differing experiences. The highest-rated item was the conduct of drills and simulations, 3.08 (SD = 1.36, Var = 1.84), while leadership resource allocation scored 2.86 (SD = 1.47, Var = 2.15), policy clarity 2.81 (SD = 1.54, Var = 2.37), staff training 2.95 (SD = 1.42, Var = 2.01), and incident response systems 2.82 (SD = 1.44, Var = 2.06). Overall, the findings suggest that KNH's cybersecurity framework is perceived as underdeveloped, particularly in resourcing, policy enforcement, staff training, and incident response, with preparedness drills viewed slightly more positively but still inconsistent.

Figure 4.9

Descriptive analysis on Proposed Framework for Cybersecurity in Healthcare at KNH.

	N	Mean	Std Dev	Var
KNH leadership actively allocates sufficient resources (budget, staff, tools) to implement cybersecurity measures.	365	2.86	1.466	2.148
KNH has established clear, enforceable cybersecurity policies that all staff are required to follow.	365	2.81	1.539	2.370
All staff at KNH receive regular, role-specific cybersecurity training that equips them to prevent cyber threats.	365	2.95	1.419	2.014
KNH has an effective, hospital-wide system for reporting and responding promptly to cybersecurity incidents.	365	2.82	1.436	2.062
KNH regularly conducts cybersecurity drills and simulations to test and improve preparedness for cyberattacks.	365	3.08	1.355	1.836
Total Avg	**365**	**2.90**	**1.44**	**2.07**

4.7 Inferential statistics

The inferential statistical analysis was conducted to examine the relationships between the key variables of the study. Correlation and regression analyses were employed to test the hypotheses and determine the strength, direction, and significance of associations among the study constructs. The use of inferential statistics enabled conclusions to be drawn beyond the sample data, providing insights into the predictive effects and interdependence within the conceptual framework. The findings formed the basis for interpreting the influence of independent variables on the dependent variable and assessing the overall model fit.

4.7.1 Correlation analysis

Correlation analysis was conducted to examine the strength, direction, and statistical significance of the relationships between the independent variables; healthcare cyber risks, the Kenya Cybercrime Act, and data protection ethical guidelines and the dependent variable, the healthcare cybersecurity framework at KNH. Statistical significance was tested at the 0.01 level to minimize the risk of Type I errors. These results provided an initial understanding of how the predictors relate to the framework and formed the basis for subsequent regression analysis, as summarized in Table 4.10.

The results show that threats in healthcare cyber risk had a weak and insignificant correlation with the cybersecurity framework ($r = 0.055$, $p = 0.297$). In contrast, the Kenya Cybercrime Act showed a weak but significant positive correlation with the framework ($r = 0.191$, $p < 0.01$), while data protection ethical guidelines had a moderate positive and significant correlation ($r = 0.294$, $p < 0.01$). Overall, the findings indicate that while cyber threats were not significantly associated with the framework, both legal and ethical measures particularly ethical guidelines showed positive relationships with the hospital's cybersecurity system.

Figure 4.10

Correlation analysis

Correlations

		Threats in Healthcare Cyber Risk	Kenya Cybercrime Act	Data Protection Ethical Guidelines	Healthcare Cyber-security Framework
Threats in Healthcare Cyber Risk	Pearson Correlation	1	.602**	.485**	.055
	Sig. (2-tailed)		.000	.000	.297
	N	365	365	365	365
Kenya Cybercrime Act	Pearson Correlation	.602**	1	.539**	.191**
	Sig. (2-tailed)	.000		.000	.000
	N	365	365	365	365
Data Protection Ethical Guidelines	Pearson Correlation	.485**	.539**	1	.294**
	Sig. (2-tailed)	.000	.000		.000
	N	365	365	365	365
Healthcare Cyber-security Framework at KNH	Pearson Correlation	.055	.191**	.294**	1
	Sig. (2-tailed)	.297	.000	.000	
	N	365	365	365	365

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

4.7.2 Regression analysis

Regression analysis was conducted to assess the joint predictive effect of healthcare cyber risks, the Kenya Cybercrime Act, and data protection ethical guidelines on the cybersecurity framework at KNH. As shown in Table 4.11, the model produced an R^2 value of 0.106, indicating that the three predictors jointly explain 10.6% of the variation in the cybersecurity framework. This suggests that while the model accounts for a modest proportion of the variance, it provides useful insights into the factors shaping cybersecurity readiness at KNH.

Figure 4.11

Regression analysis model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.326[a]	.106	.099	.77301

a. Predictors: (Constant), Data Protection Ethical Guidelines at KNH, Threats in Healthcare Cyber Risk at KNH, Kenya Cybercrime Act

4.7.3 Regression analysis Anova

The ANOVA results in Table 4.12 show that the regression model significantly predicts the healthcare cybersecurity framework at KNH, $F(3, 361) = 14.267$, $p < 0.001$. This confirms that the independent variables cyber risks, the Kenya Cybercrime Act, and ethical guidelines jointly contribute significantly to explaining variations in the cybersecurity framework.

Figure 4.12

Regression analysis Anova

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	25.576	3	8.525	14.267	.000[b]
	Residual	215.714	361	.598		
	Total	241.290	364			

a. Dependent Variable: Healthcare Cyber-security Framework at KNH

b. Predictors: (Constant), Data Protection Ethical Guidelines at KNH, Threats in Healthcare Cyber Risk at KNH, Kenya Cybercrime Act

4.7.4 Regression analysis coefficients

Table 4.14 presents the regression coefficients for the predictors of the cybersecurity framework at KNH. The results show that healthcare cyber risks had a significant negative effect ($B = –0.182$, $p = 0.007$), indicating that increased threats reduce the effectiveness of the framework. The Kenya Cybercrime Act had a positive but marginally insignificant effect ($B = 0.136$, $p = 0.054$). Data

protection ethical guidelines had the strongest and significant positive influence (B = 0.303, p < 0.001), making them the most important predictor of the framework. The regression constant was 1.893 (p < 0.001).

Table 4.13

Regression analysis coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.893	.249		7.611	.000
	Threats in Healthcare Cyber Risk at KNH	-.182	.068	-.173	-2.689	.007
	Kenya Cybercrime Act	.136	.070	.129	1.935	.054
	Data Protection Ethical Guidelines at KNH	.303	.060	.309	5.070	.000

a. Dependent Variable: Healthcare Cyber-security Framework at KNH

4.8 Chapter Summary

This chapter presented the results of the study based on data from 365 respondents at Kenyatta National Hospital. Descriptive analysis highlighted high perceptions of cyber risks, moderate recognition of the Kenya Cybercrime Act's role, and generally positive views of ethical data protection practices, while the existing cybersecurity framework was rated as underdeveloped. Correlation analysis showed that cyber risks were not significantly related to the framework, whereas the Kenya Cybercrime Act and ethical guidelines were positively associated. Regression results indicated that the three predictors jointly explained 10.6% of the variation in the cybersecurity framework, with ethical guidelines emerging as the strongest positive predictor, cyber risks having a significant negative effect, and the Kenya Cybercrime Act showing a marginal influence. Overall, the findings point to the critical role of ethical practices and the need for

strengthened legal enforcement and proactive risk management in enhancing cybersecurity resilience at KNH.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter summarizes the study findings and interprets them in relation to the research objectives and existing literature. It also presents conclusions, policy recommendations, and practical measures for improving cybersecurity in Kenyan healthcare institutions, with Kenyatta National Hospital (KNH) as the focus. The discussion is organized around the four objectives: identifying cyber threats, evaluating the Kenya Cybercrime Act, assessing ethical data protection guidelines, and proposing a cybersecurity framework. The Socio-Technical Systems (STS) Theory is used to interpret the findings, and the chapter concludes with recommendations for future research.

5.2 Summary of Findings

The study sought to examine healthcare cyber risks and countermeasures at Kenyatta National Hospital (KNH), focusing on threats, the role of the Kenya Cybercrime Act, ethical data protection guidelines, and the development of a cybersecurity framework. Using a descriptive research design, data were collected from 365 staff drawn from clinical, ICT, and records departments, achieving a 100% response rate. Most respondents were male (54.5%), aged 31–40 years (42.5%), held undergraduate degrees (50.1%), and had 6–10 years of work experience (41.6%), ensuring broad representation of hospital staff perspectives.

Findings on the first objective showed high awareness of cyber risks, with external attacks rated the most critical (M = 4.18), followed by poor risk assessment (M = 4.04), vulnerable medical systems (M = 3.99), insider threats (M = 3.92), and operational disruptions (M = 3.88). Correlation analysis revealed no significant association between cyber risks and the cybersecurity framework

(r = 0.055, p = 0.297), while regression confirmed a significant negative effect (B = -0.182, p = 0.007).

On the second objective, staff perceived the Cybercrime Act as beneficial, particularly in building patient trust (M = 4.06), improving awareness of legal provisions (M = 4.05), and informing hospital policy (M = 3.97). The Act showed a weak but statistically significant positive correlation with the cybersecurity framework (r = 0.191, p < 0.01), and regression revealed a marginally significant positive effect (B = 0.136, p = 0.054).

The third objective revealed that ethical data protection practices were generally upheld, with the highest ratings for enforcing confidentiality, integrity, and availability principles (M = 4.01) and regular staff training (M = 3.98). Ethical guidelines showed a moderate positive correlation with the cybersecurity framework (r = 0.294, p < 0.01) and emerged as the strongest predictor in regression (B = 0.303, p < 0.001; β = 0.309).

Finally, in addressing the fourth objective, evaluation of KNH's cybersecurity practices showed moderate maturity, with simulation drills scoring highest (M = 3.08) and incident response the lowest (M = 2.82). These findings informed the proposal of a socio-technical cybersecurity framework built around four pillars: policy institutionalization, leadership commitment, human-technology synergy, and feedback-driven evolution, offering a scalable and context-specific model for Kenya's public healthcare sector.

5.3 Discussion of findings

5.3.1 Threats in healthcare cyber risk at Kenyatta National Hospital.,

The findings under the first objective revealed a strong perception among respondents that Kenyatta National Hospital (KNH) faces critical cybersecurity threats across multiple dimensions.

Of all the risks examined, external cyberattacks were viewed as the most severe, with a mean rating of 4.18. This underscores an acute awareness of threats such as ransomware, phishing, and distributed denial-of-service (DDoS) attacks, which have become increasingly prevalent within healthcare environments globally. Respondents at KNH recognized that the hospital's extensive patient records, interconnected systems, and digital infrastructure make it a prime target for sophisticated cybercriminals. This perception aligns with the Socio-Technical Systems (STS) Theory, which emphasizes the interdependence between technological systems and the human agents interacting with them. A failure to secure either component can compromise the entire network. The finding echoes research by Ghafur et al. (2022), who highlighted that external attacks have caused significant disruptions in UK hospitals, often resulting in the unavailability of clinical systems. Similarly, Schmeelk et al. (2021) reported that over 30 million people in the United States were affected by healthcare-related cyberattacks in 2020 alone, illustrating the widespread nature of this threat. Locally, Ochieng and Ojwang (2020) observed that Kenya's leading public hospitals are particularly vulnerable due to gaps in perimeter defenses and limited incident response capabilities. These studies reinforce the respondents' concern that KNH's cyber resilience is under growing external pressure and must be strengthened urgently through both technological safeguards and user preparedness.

Closely related to this concern is the perceived inadequacy of risk assessment and monitoring, which scored a mean of 4.04. Participants indicated that KNH lacks sufficient systems for real-time threat detection, periodic vulnerability scanning, and structured risk mitigation protocols. This limitation is particularly worrying because it suggests the hospital is often unaware of threats until after they have materialized, reinforcing a reactive rather than proactive security posture. From the STS perspective, this reflects an imbalance in the system, where technology may exist,

but without the supporting human processes such as continuous training, analysis, and feedback loops, the system fails to evolve in step with emerging risks. The need for continuous monitoring and a standardized cybersecurity architecture is emphasized in the NIST Cybersecurity Framework (NIST, 2017b), which advocates for consistent risk assessments as foundational to cyber defense. Hubbard and Seiersen (2023) further argue that failure to institutionalize cyber risk management leads to unpredictable vulnerabilities. Supporting this view in the Kenyan context, Mutinda and Ongus (2020) showed that public health institutions with proactive monitoring frameworks report significantly fewer security incidents than those that rely on post-incident corrections. Therefore, the lack of structured risk oversight at KNH represents a critical deficiency that, if unaddressed, may compromise all other efforts in cybersecurity.

A similarly pressing issue identified was the vulnerability of medical devices and digital systems, with a mean rating of 3.99. Many hospital systems, particularly those linked to diagnostics and patient monitoring, run on outdated software or lack adequate authentication mechanisms. Respondents expressed concern that these weaknesses not only expose sensitive patient data but also pose direct risks to patient care, especially when critical equipment can be disabled or manipulated remotely. This view once again reflects the STS theory's assertion that an effective security strategy must integrate both human and machine processes. Technological solutions must be accompanied by a culture of accountability and systems thinking. Studies by Wurm et al. (2017) and Lou et al. (2020) show that Internet of Medical Things (IoMT) devices are particularly susceptible to exploitation when not supported by strong firmware and update mechanisms. Tokognon et al. (2017) also found that hospitals that rely on legacy systems are more frequently targeted by attackers who exploit unpatched vulnerabilities. Given that KNH manages high patient volumes and complex procedures, any breach in medical systems could be catastrophic

highlighting the need for updated technologies, routine patching, and clear device management policies.

The issue of insider threats followed closely, with a mean score of 3.92, revealing a significant concern about the actions or negligence of internal personnel. This includes unauthorized access to patient files, mishandling of login credentials, and failure to follow security protocols. The respondents' concern is warranted, as insider threats often bypass technical defenses due to the legitimate access these users have. The STS framework sheds light on this issue by pointing out that vulnerabilities often emerge when organizations fail to address the human behaviours that intersect with technology. Cybersecurity is not merely a technical problem but a social one, as noted by Malatji et al. (2019), where employees' actions are deeply embedded in the broader institutional culture. Abdullah et al. (2020) found that weak training and accountability mechanisms in African hospitals often lead to inadvertent internal breaches. In parallel study, Xu et al. (2019) reported that U.S. healthcare staff who lacked cybersecurity training were more likely to cause accidental data leaks. Almutairi et al. (2020) emphasized that insider threats are particularly difficult to detect, requiring not just technological monitoring but also trust-building and ethical education among staff. Thus, reducing insider risk at KNH demands stronger internal controls, regular awareness campaigns, and access management policies tailored to specific roles.

Although operational disruptions resulting from cyber incidents were rated the lowest among the five areas (mean = 3.88), this finding should not be dismissed. Respondents acknowledged that even temporary system failures could interrupt admissions, delay diagnostics, or affect patient referrals challenges that are particularly impactful in a high-demand hospital like KNH. The lower rating may reflect staff desensitization to intermittent downtimes or a lack of visibility into system-wide dependencies. Nevertheless, this threat remains serious because it directly affects patient

outcomes. The STS theory reiterates that technological interruptions can ripple across the social fabric of the organization, undermining teamwork, communication, and clinical judgment. Weerasinghe et al. (2020) found that operational downtime caused by cyber incidents leads to measurable declines in healthcare performance, especially in emergency departments. Wyatt (2021) reported that African hospitals often fail to quantify the costs of such interruptions, leading to underinvestment in IT resilience. Schlosberg (2021) similarly cautioned that disruptions in digital infrastructure erode both public trust and operational efficiency, particularly in referral canters where care coordination is critical. The findings therefore reinforce the argument that operational resilience should be an integral part of any cybersecurity framework at KNH, with failover systems, regular backups, and continuity protocols in place.

In addition to the descriptive insights, inferential statistics revealed a critical and statistically significant relationship between perceived threats in healthcare cyber risk and the effectiveness of the healthcare cybersecurity framework at KNH. Regression analysis showed a negative unstandardized coefficient for threats in healthcare cyber risk ($B = -0.182$, $p = 0.007$). This finding indicates that as perceptions of cyber threats increase, confidence in the effectiveness of KNH's cybersecurity framework decreases. In other words, heightened threat awareness is associated with reduced belief in the institution's capacity to manage those risks effectively. The negative direction of the relationship underscores a potentially serious gap: while threats are clearly recognized by hospital staff, the institutional response in terms of cybersecurity infrastructure is not perceived to be adequately responsive or protective.

This interpretation is further supported by the correlation analysis, which revealed that the relationship between threats in healthcare cyber risk and the cybersecurity framework was statistically insignificant ($r = 0.055$, $p = 0.297$). This lack of correlation, despite the high perceived

threat levels, suggests a disconnect between risk perception and organizational readiness. Together, the regression and correlation findings highlight that while KNH personnel are aware of the dangers they face, there is limited confidence in the systems designed to mitigate those risks. This reinforces the need for KNH to strengthen not only its cybersecurity architecture but also the visibility, trustworthiness, and operational maturity of that framework among its workforces.

5.3.2 Kenya cybercrime Act on healthcare cyber risks at KNH

The analysis of the second objective sought to examine the impact of the Kenya Cybercrime Act as a national legal framework in supporting cybersecurity practices at Kenyatta National Hospital (KNH). The findings revealed broad agreement among respondents that the Act plays a critical role in enhancing data protection and shaping organizational behaviour in managing cyber risks. The statement receiving the highest level of agreement was that staff were aware of the provisions of the Kenya Cybercrime Act, which recorded a mean of 4.05 (SD = 1.10). This indicates that a significant proportion of KNH staff are informed about the law's requirements, including provisions around unauthorized access, system interference, and criminal liability for cybercrime. This awareness reflects a deterrent effect, best explained by Deterrence Theory, which posits that individuals are less likely to engage in misconduct when laws are clearly articulated, perceived as legitimate, and backed by the threat of sanctions. The Kenya Cybercrime Act, in this context, functions as both a regulatory and behavioural instrument. This finding aligns with studies such as Choi et al. (2020), which demonstrated that cyber law awareness significantly decreases internal abuse of information systems. Similarly, Kaplan et al. (2019) noted that well-informed employees are more likely to adhere to security standards, especially in regulated environments.

In tandem with legal awareness, respondents strongly agreed that the Cybercrime Act enhances patient trust in healthcare data systems, scoring a mean of 4.06 (SD = 1.12). This suggests that

visible legal protections positively influence how patients perceive the confidentiality and integrity of their personal data. From a theoretical standpoint, this finding also connects to Deterrence Theory, which posits that the existence of enforceable laws not only dissuades misconduct but also assures stakeholders such as patients that breaches are less likely to occur. Trust, in this regard, becomes a derivative benefit of legal enforcement. Supporting this, Almutairi et al. (2020) found that in healthcare institutions where data protection laws are publicly communicated and enforced, patients report greater confidence in sharing personal information. The Kenya Cybercrime Act, therefore, serves as a legal boundary that reinforces trust in the institution's digital infrastructure.

Another important finding was that KNH has integrated the Kenya Cybercrime Act into its policies and procedures, with a mean score of 3.97 (SD = 1.10). This implies that the hospital has taken deliberate steps to institutionalize the provisions of the Act within its internal frameworks such as user access policies, incident response procedures, and system audit controls. This development aligns closely with Institutional Theory, which explains how organizations adapt their structures and routines to conform with external pressures, including legal mandates. By aligning its operations with national cybersecurity legislation, KNH demonstrates normative and regulatory compliance, a key aspect of institutional legitimacy. Elshenawy et al. (2021) assert that hospitals that formalize their alignment with national laws achieve better internal security outcomes and regulatory ratings. In the Kenyan context, the Communications Authority (2020) has also emphasized the necessity of localizing cybersecurity legislation at the institutional level, a principle evidently reflected in KNH’s practices.

A closely related finding was that the Cybercrime Act has strengthened legal protections for patient data, with a mean score of 3.95 (SD = 1.13). Respondents agreed that the law creates clear criminal liability for unauthorized access and data tampering, thereby improving institutional

accountability. Like previous items, this finding reflects Deterrence Theory in action, wherein legal consequences shape staff behaviour and elevate the seriousness with which data protection is treated. It also aligns with Institutional Theory, in that legal structures have influenced KNH's operational culture and reinforced formal expectations about data handling. Ponemon Institute (2016) found comparable results, noting that healthcare organizations in jurisdictions with clear legal penalties for breaches tend to adopt stricter data governance measures.

The statement that the Cybercrime Act has contributed to reducing cyber incidents also received a high mean of 3.95 (SD = 1.04). This indicates that staff perceive a practical benefit from the law in terms of reducing events such as phishing, unauthorized data access, or malicious intrusions. The decrease in perceived incidents can be interpreted through the lens of Socio-Technical Systems Theory, which emphasizes that security outcomes depend on the effective interaction between human behaviour (shaped by awareness and fear of legal consequence) and technical systems (configured to align with legal requirements). This finding supports the idea that legal frameworks, when internalized and enforced through institutional systems, become an embedded part of a broader cybersecurity ecosystem. Studies by Weerasinghe et al. (2020) and Schlosberg (2021) confirm that strong legal frameworks contribute to behavioural change and improved system use, thus reducing vulnerability.

Turning to the inferential results, correlation analysis revealed a moderate, positive, and statistically significant relationship between the perceived impact of the Kenya Cybercrime Act and the strength of the cybersecurity framework at KNH ($r = 0.191$, $p < 0.01$). This indicates that as staff perceive the Cybercrime Act to be effective, their confidence in the hospital's overall cybersecurity systems also improves. This aligns with both Institutional Theory and Socio-Technical Systems Theory, suggesting that institutional security improves not only through the

presence of legal mandates but also through their integration into both policy and practice. Further support is provided by regression analysis, where the Cybercrime Act exhibited a positive, though marginally significant influence on the cybersecurity framework (B = 0.136, p = 0.054). Although the relationship narrowly missed the conventional 0.05 significance threshold, its standardized coefficient (β = 0.129) implies that the Act still plays a meaningful, if moderate, role in shaping KNH's institutional defense systems. This is consistent with Institutional Theory, in that legal frameworks contribute to shaping organizational form and operational routines, and with STS Theory, by highlighting how legal structures interact with staff awareness and technical implementation to improve cybersecurity outcomes.

Together, these findings confirm that the Kenya Cybercrime Act not only provides legal protections but also serves as a regulatory influence on institutional behaviour and system design at KNH. The integration of the Act into both policy and perception underscores the critical role of law in healthcare cybersecurity governance.

5.3.3 Data protection ethical guidelines on Healthcare Cybersecurity risks at KNH.

The findings related to data protection ethical guidelines at Kenyatta National Hospital (KNH) demonstrate a strong institutional emphasis on ethical behaviour in safeguarding patient information. Among the examined items, the highest-rated practice was the implementation of the principles of confidentiality, integrity, and availability through mechanisms such as secure login systems, restricted access to sensitive data, and regular data backups. This item received a mean score of 4.01 (SD = 1.19), suggesting widespread agreement among respondents that KNH prioritizes ethical control of digital information. This practice aligns with the Socio-Technical Systems (STS) Theory, which posits that robust cybersecurity requires alignment between technological safeguards and ethical human behaviour. These technical-environmental controls

are supported by routine training and institutional policy enforcement, thus enabling the ethical dimension of data protection to be realized within a working system. The implementation of these principles mirrors observations by Lee & Smith (2023), who asserted that system design and ethical culture must be integrated to ensure resilience in data handling. Roberts and Anderson (2023) similarly observed that confidentiality and role-based access controls significantly reduce data exposure risks in hospital networks. Zhou and Tang (2021) emphasized that technical ethics mechanisms such as authentication and redundancy ensure compliance and mitigate human error, a concept evident in the practices at KNH.

Closely following this was the finding that KNH provides regular training to staff on ethical standards, which achieved a mean score of 3.98 (SD = 1.18). This indicates that hospital personnel are periodically educated on key ethical issues including confidentiality, informed consent, and professional data handling. The relevance of this finding is best interpreted through the lens of Institutional Theory, which emphasizes that formal rules, norms, and values are embedded within organizations to enhance legitimacy and compliance. Training is a vital normative tool through which ethical standards are institutionalized, making them an expected and shared part of organizational behaviour. Studies by Johnson & Becker (2022) highlight how recurring training fosters ethical commitment and reduces internal violations. Alahmari et al. (2023) further argued that ethical training helps transform awareness into embedded behaviour, especially in clinical settings where information flows rapidly. In the Kenyan context, such efforts are critical for aligning healthcare practice with both national policy and international privacy standards, reinforcing the importance of institutionalized ethics.

Another significant finding was that KNH enforces disciplinary action for ethical violations, such as unauthorized access to records or negligent disclosure of patient information. This item scored

3.97 (SD = 1.18), demonstrating strong agreement that there are consequences for unethical conduct. This is clearly aligned with Deterrence Theory, which posits that the presence of credible sanctions discourages individuals from engaging in violations. When staff are aware that ethical breaches have tangible repercussions, their likelihood of engaging in such behaviour diminishes. This is particularly important in high-risk environments like hospitals, where data sensitivity is paramount. Supporting this interpretation, Martin and Williams (2022) found that ethical misconduct in healthcare organizations declined when clear punitive structures were in place. Similarly, Perakslis (2014) emphasized that deterrent mechanisms must be consistently enforced to support a sustainable culture of privacy and accountability.

The finding that patients are informed of how their data is managed, with a mean of 3.93 (SD = 1.15), indicates the hospital's effort to promote transparency and informed consent which are key pillars of ethical data management. This again resonates with Institutional Theory, which emphasizes that ethical legitimacy is shaped by external expectations, including patient rights and legal mandates. Informing patients of how their data is used and who can access it not only meets legal obligations but also strengthens the ethical relationship between healthcare providers and service users. Literature supports this approach: Kumar and Singh (2023) found that patients are more cooperative and satisfied with care when their rights are acknowledged and protected. Smith and Jones (2020) also noted that hospitals with strong patient communication protocols reported fewer complaints and higher levels of trust in digital systems.

The lowest-scoring item among the examined ethical practices was the existence of a documented code of ethics governing access, storage, and sharing of patient data, with a mean score of 3.83 (SD = 1.17). While still reflecting general agreement, this result suggests some variability in staff awareness or understanding of the code. From a Socio-Technical Systems perspective, the

presence of an ethical code must be complemented by technological tools and clear dissemination strategies. A code of ethics that exists only in documentation, without integration into workflows and systems, may fail to produce the intended behavioural outcomes. Research by Almutairi et al. (2020) affirms this by showing that ethical guidelines are most effective when combined with digital policies and technical restrictions. Meanwhile, Elshenawy et al. (2021) argue that codes of conduct become operationally meaningful only when they are embedded within user interfaces, data access routines, and staff performance reviews. Thus, although KNH has taken steps to establish ethical norms, greater clarity, visibility, and integration of these norms across hospital systems would enhance their effectiveness.

These descriptive findings are strongly supported by inferential statistics. Regression analysis identified data protection ethical guidelines as the strongest predictor of the cybersecurity framework at KNH, with a standardized coefficient (β) of 0.309 and unstandardized coefficient B = 0.303 ($p < 0.001$). This statistically significant positive relationship confirms that stronger ethical controls and practices directly improve the hospital's cybersecurity posture. The result validates the theoretical premise of the Socio-Technical Systems Theory, which holds that security is most effective when organizational ethics and technical safeguards co-evolve. In the same regression model, data protection ethics outperformed both legal and risk variables in explaining variance in the cybersecurity framework highlighting its critical influence.

The correlation analysis further supported this relationship, showing a moderate and statistically significant association ($r = 0.294$, $p < 0.01$) between ethical guidelines and the cybersecurity framework. This suggests that as ethical standards become more embedded, confidence in KNH's cybersecurity systems also improves. This relationship reflects both Institutional and STS

perspectives, as ethical standards, when formally established and practically implemented become institutionalized and positively affect user behaviour and system performance.

Taken together, these results affirm that ethical data protection practices at KNH are a cornerstone of its cybersecurity efforts. Ethical guidelines are not only recognized by staff but also actively shape behaviour, influence technical configuration, and improve institutional trust in cybersecurity mechanisms. As the strongest predictor in the study, they form a critical foundation for building resilient, trustworthy, and effective digital healthcare systems.

5.3.4 Framework for the establishment of cybersecurity measures in healthcare at KNH.

The assessment of the healthcare cybersecurity framework at Kenyatta National Hospital (KNH) revealed important insights into existing strengths, limitations, and areas for targeted improvement. Across five key dimensions (resource allocation, policy clarity, staff training, incident response, and simulation preparedness) the results reflect a moderate perception of cybersecurity maturity, pointing to the need for a more structured and integrated model for cybersecurity implementation.

The item with the highest mean score was KNH's practice of conducting cybersecurity drills and simulations, which recorded a mean of 3.08 (SD = 1.36). While still below the threshold of high agreement, this relatively stronger response suggests that the hospital has taken initial steps toward preparedness through testing and scenario planning. These exercises are essential in identifying weaknesses in response mechanisms and reinforcing staff behavior under simulated threat conditions. This finding aligns directly with Socio-Technical Systems (STS) Theory, which emphasizes that both technical capacity (e.g., drills, simulations) and social responsiveness (e.g., how staff act in emergencies) must function cohesively for a system to withstand external threats. As noted by Ashrafi et al. (2022), simulation-based training is an effective method to enhance

human–system interaction, particularly in high-stakes environments like healthcare where prompt response is key to maintaining data integrity and patient safety.

Slightly below this was the finding that KNH provides regular, role-specific cybersecurity training, with a mean score of 2.95 (SD = 1.42). This suggests an uneven implementation of training programs, where some staff receive adequate instruction while others may be underserved. Given that a substantial portion of respondents expressed uncertainty in identifying security threats, the variability in responses reflects gaps in knowledge dissemination. According to STS Theory, technical tools must be accompanied by human competence; without sufficient training, even the best technological defenses can be undermined by human error. Recent studies by Alameri et al. (2023) and Kane and Skibinski (2021) emphasize that continuous, role-specific education is foundational to enhancing cybersecurity literacy and fostering a proactive security culture.

The statement that KNH leadership actively allocates sufficient resources including budget, staffing, and technical tools for cybersecurity received a mean score of 2.86 (SD = 1.47). This finding reflects moderate concern among staff regarding leadership commitment and institutional investment. In many public healthcare settings, limited resources and competing priorities hinder substantial investments in digital security. Within the STS framework, inadequate investment disrupts the integration of technical infrastructure with organizational objectives, undermining overall security. Kimani and Wanjiru (2023) have highlighted that insufficient funding remains a critical barrier in Kenyan public hospitals, while Kane and Skibinski (2021) stress the importance of leadership engagement in fostering sustainable cybersecurity practices.

A comparable result was observed for the item stating that KNH has clear and enforceable cybersecurity policies for all staff, which garnered a mean score of 2.81 (SD = 1.54). The low agreement and high variability suggest inconsistency in either the communication or enforcement

of these policies. From an STS perspective, the existence of technical policies that are not fully internalized by personnel points to a breakdown in the institutional embedding of norms and procedures. As Malatji et al. (2019) argue, cybersecurity rules and roles must be well defined and consistently reinforced within an organization's culture; otherwise, the policies risk being treated as mere formalities rather than as active components of daily operations.

The lowest-rated item in the evaluation was the effectiveness of KNH's hospital-wide system for reporting and responding to cybersecurity incidents, with a mean score of 2.82 (SD = 1.44). This finding indicates critical weaknesses in the institution's incident response infrastructure. Whether due to the lack of user-friendly reporting tools, vague reporting procedures, or delayed response times, the perceived ineffectiveness in this area constitutes a major vulnerability. Within the STS framework, an effective incident response system requires seamless integration of social factors such as clear communication channels and staff empowerment with advanced technical tools like intrusion detection and logging systems. Whitman and Matto'd (2021) have shown that fragmented incident response processes often leave organizations exposed to prolonged cyber breaches, consequently endangering both data security and patient care.

Although inferential statistics specific to this objective were not computed separately, broader regression analyses in the study indicate that elements such as ethical guidelines and threat perceptions significantly predict the robustness of the cybersecurity framework. These results further support the STS position that successful cybersecurity is not achieved by technical controls alone, but rather through the concerted alignment of institutional policies, leadership commitment, human behaviour, and technical infrastructure.

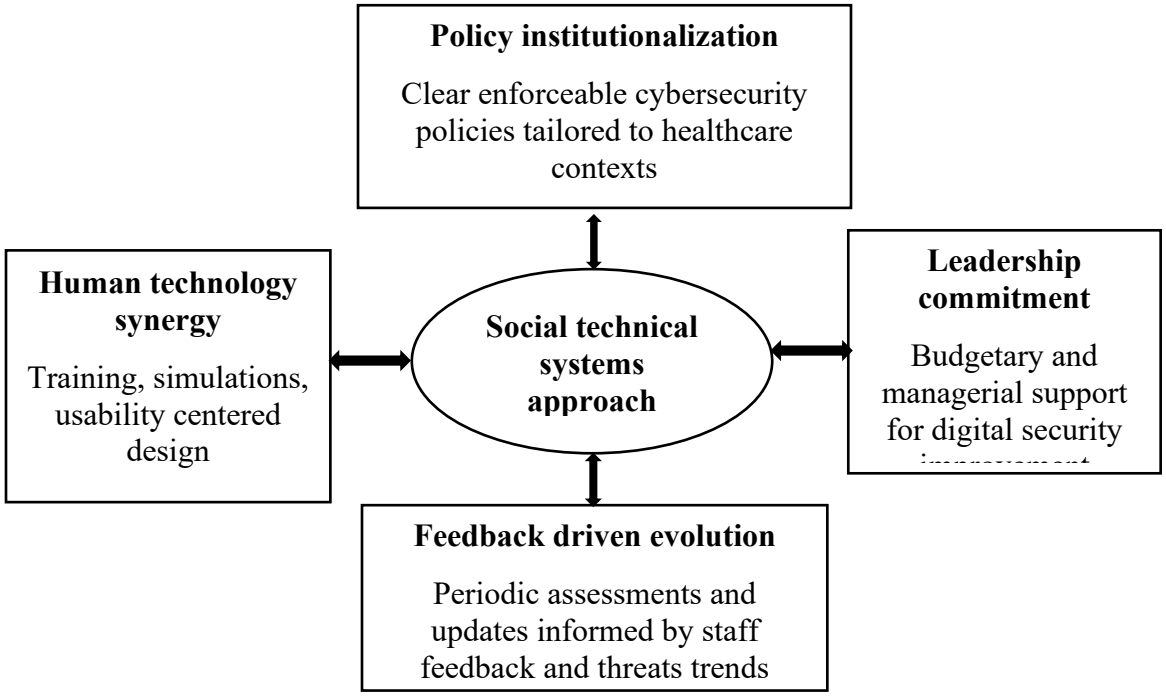
Together, the findings show that while KNH demonstrates growing attention to cybersecurity, significant gaps remain in areas such as resource allocation, training, policy enforcement, and

incident response. Guided by the Socio-Technical Systems (STS) Theory, a comprehensive cybersecurity framework for Kenyan healthcare should therefore be built on four key pillars: (1) Policy institutionalization, involving the development, communication, and strict enforcement of healthcare-specific cybersecurity policies; (2) Leadership commitment, through sustained resource allocation and strategic oversight; (3) Human–technology synergy, achieved by continuous, role-based training and simulation exercises; and (4) Feedback-driven evolution, where measures are regularly updated based on incident reviews, new threat intelligence, and technological progress.

Figure 5.1

Framework for the establishment of cybersecurity measures in healthcare at KNH

.



5.4 Conclusions

This section presents the conclusions drawn from the study based on the four specific objectives. The conclusions are grounded in the data collected, analysed, and discussed in the previous

chapters, and they reflect the realities and experiences of cybersecurity implementation in a large public healthcare institution in Kenya. Each objective is addressed individually to provide a focused summary of the study's key findings and their implications. These conclusions offer insights into how various dimensions of cyber risk, legal infrastructure, ethical governance, and organizational preparedness influence the effectiveness of cybersecurity in the healthcare sector.

The first objective sought to examine the threats in healthcare cyber risk at Kenyatta National Hospital., The findings revealed that respondents perceived external cyberattacks, weak risk assessment mechanisms, and vulnerabilities in medical devices as significant threats to the hospital's digital infrastructure. Insider threats and operational disruptions were also noted, though to a slightly lesser extent. The study concludes that while staff are acutely aware of the cybersecurity risks facing the institution, this awareness is not matched by confidence in the hospital's existing cyber defenses. Regression analysis showed a statistically significant negative effect of threat perception on the perceived strength of the cybersecurity framework. This implies that heightened awareness of threats corresponds with diminished trust in the institution's capacity to manage those risks, emphasizing a critical need for systemic improvements.

The second objective analysed the impact of the Kenya Cybercrime Act on cybersecurity at KNH. The study concluded that the Act plays a supportive but under-leveraged role in enhancing institutional security. While staff showed strong awareness of the law and acknowledged its contribution to building patient trust and protecting data, its predictive influence on cybersecurity outcomes was only marginally significant. This suggests that although the legal framework provides a necessary foundation for cybersecurity, its institutional effectiveness depends on consistent enforcement, staff training, and better integration into internal policies and practices.

Therefore, legislative support alone is insufficient without corresponding organizational commitment and implementation.

With respect to data protection ethical guidelines, the study found that they were the most influential predictor of the strength of the cybersecurity framework. Staff agreed that ethical principles such as confidentiality, integrity, and accountability were well understood and partially enforced. Regular training and disciplinary measures were also in place, albeit inconsistently. The conclusion drawn is that ethical norms play a foundational role in sustaining secure digital environments in healthcare. When these guidelines are well-communicated and embedded in practice, they promote responsible system use and help bridge gaps left by technological or legal limitations. Thus, a values-driven approach to cybersecurity is critical for institutional resilience.

Finally, the study proposed a framework for establishing effective cybersecurity in the healthcare sector, informed by the evaluation of KNH's practices. The analysis of five operational areas—simulation preparedness, training, resource allocation, policy enforcement, and incident response revealed moderate levels of maturity, with simulation drills being the most developed and incident response the weakest. The conclusion is that cybersecurity at KNH, and similar public healthcare institutions, requires a more integrated and structured model. This model should align leadership, policy, training, and technology under a unified strategy grounded in Socio-Technical Systems (STS) Theory. Such an approach ensures that both human and technical factors work in synergy to protect patient data and institutional integrity.

In summary, the study highlights the urgent need for a balanced, people-cantered, and systems-oriented cybersecurity approach within Kenyan healthcare institutions. Enhancing legal enforcement, deepening ethical practice, improving training and policy adherence, and securing leadership commitment will be central to achieving long-term cybersecurity resilience.

5.5 Recommendations

Based on the study findings and conclusions, the following recommendations are proposed to strengthen healthcare cybersecurity at Kenyatta National Hospital and similar public institutions in Kenya:

5.5.1 Recommendation for practice

1. Strengthen Institutional Cybersecurity Infrastructure in Response to Perceived Threats

The study found that external cyberattacks, weak risk assessment, and system vulnerabilities are among the most significant threats perceived by KNH staff. However, the lack of confidence in the hospital's cybersecurity framework suggests a disconnect between threat awareness and institutional preparedness.

- **Recommendation:** KNH should prioritize the development and deployment of a robust, layered cybersecurity infrastructure. This should include real-time intrusion detection systems, regular vulnerability assessments, and periodic audits of medical devices and digital health systems.
- **Implementation:** Develop a dedicated cybersecurity operations unit within the ICT department, staffed with skilled personnel, and supported with adequate resources.

2. Enhance the Operationalization of the Kenya Cybercrime Act within Institutional Policies

While staff demonstrated strong awareness of the Kenya Cybercrime Act and appreciated its relevance, its impact on KNH's cybersecurity framework was only marginally significant.

- **Recommendation:** KNH should formally integrate the provisions of the Kenya Cybercrime Act into internal cybersecurity policies, procedures, and staff codes of conduct.
- **Implementation:** Conduct annual legal awareness workshops and revise institutional ICT policies to directly reference key provisions of the Act, such as penalties for unauthorized access, data tampering, and non-compliance.

3. Institutionalize Ethical Guidelines and Scale Up Role-Based Cybersecurity Training

Ethical data protection guidelines were identified as the strongest predictor of an effective cybersecurity framework. However, inconsistencies in training and partial enforcement were noted.

- **Recommendation:** KNH should institutionalize ethical guidelines by embedding them into everyday workflows, onboarding protocols, and performance appraisals. Comprehensive, role-specific training should be offered consistently across all departments.
- **Implementation:** Develop an e-learning module on healthcare data ethics, tailored to job functions (e.g., clinicians, IT staff, administrative personnel), and make certification mandatory on an annual basis.

4. Increase Executive Commitment and Budget Allocation for Cybersecurity Programs

The study revealed low staff confidence in leadership's commitment to cybersecurity, especially in resource allocation and strategic prioritization.

- **Recommendation:** The hospital's leadership should formally prioritize cybersecurity as a strategic institutional goal and allocate adequate budget for both technical and human capacity development.
- **Implementation:** Include cybersecurity as a standing item in senior management meetings and integrate it into the hospital's five-year strategic plan.

5. Improve Incident Reporting and Response Systems

The lowest-scoring item in the study was the perceived effectiveness of the incident response system, indicating weak mechanisms for reporting, escalation, and mitigation.

- **Recommendation:** KNH should develop and publicize a formal cybersecurity incident response plan (CIRP), supported by user-friendly reporting tools and clear escalation procedures.
- **Implementation:** Create a centralized incident reporting portal with real-time alerts, automated triaging, and anonymous reporting options to encourage openness and quick resolution.

6. Adopt a Socio-Technical Cybersecurity Framework

The findings support a socio-technical approach, emphasizing that effective cybersecurity depends on the integration of technology, human behaviour, and institutional culture.

- **Recommendation:** KNH and other healthcare providers should adopt a cybersecurity framework grounded in Socio-Technical Systems (STS) Theory, emphasizing balanced investment in people, processes, and platforms.
- **Implementation tip:** Use the study's proposed framework with four pillars (Policy Institutionalization, Leadership Commitment, Human-Technology Synergy, and Feedback-Driven Evolution) as a blueprint for continuous improvement.

5.5.2 Recommendation for future studies

Based on the findings and limitations of this study, two key areas are recommended for future research, as they address substantial gaps that emerged from the data analysis and interpretation.

The first area concerns the observed disconnect between high staff awareness of cyber threats and the limited confidence in the effectiveness of the existing cybersecurity framework at Kenyatta National Hospital., Despite respondents demonstrating strong knowledge of cyber risks such as external attacks, insider threats, and systemic vulnerabilities, this awareness did not significantly correlate with their perception of institutional preparedness. This gap suggests that knowledge alone does not necessarily lead to practical improvements in cybersecurity implementation. Future research should therefore investigate the organizational, cultural, or structural barriers that may hinder the translation of cyber risk awareness into actionable institutional reforms. Such studies could explore factors such as leadership responsiveness, bureaucratic constraints, staff empowerment, and interdepartmental coordination. Understanding this gap would be instrumental in developing more effective, system-wide strategies that move beyond awareness campaigns and toward tangible cyber resilience in public healthcare institutions.

The second area for further study relates to the practical enforcement and institutional impact of the Kenya Cybercrime Act within the healthcare sector. While this study found that staff were highly aware of the Act and acknowledged its relevance in enhancing patient trust and defining legal protections, its actual influence on the cybersecurity framework at KNH was only marginally significant. This raises questions about how well the Act has been operationalized at the institutional level. Future research should critically examine the extent to which public hospitals have internalized the provisions of the Kenya Cybercrime Act into their internal policies, reporting systems, and staff accountability mechanisms. In addition, such studies could assess how regulatory agencies monitor compliance and whether breaches are prosecuted or lead to corrective action. This line of inquiry is crucial for determining whether national cybersecurity legislation has meaningful enforcement power in the healthcare sector or remains symbolic in practice.

By addressing these two gaps, future research can contribute to a deeper understanding of the socio-institutional dynamics that affect cybersecurity performance in public health settings. These insights will not only enrich academic literature but also guide policymakers, hospital administrators, and legal authorities in crafting more effective, enforceable, and context-sensitive cybersecurity strategies.

5.6 Chapter summary

This chapter presented the summary of the study findings, discussed the results in relation to each research objective, drew conclusions based on both descriptive and inferential analyses, and provided recommendations informed by empirical evidence. The chapter focused on examining healthcare cybersecurity at Kenyatta National Hospital (KNH) through four specific lenses: identifying prevalent threats, evaluating the impact of the Kenya Cybercrime Act, assessing ethical

data protection practices, and proposing a cybersecurity framework grounded in the Socio-Technical Systems (STS) Theory.

The findings showed that KNH faces significant cyber risks, with external attacks and system vulnerabilities being particularly prominent. While staff demonstrated awareness of these risks, confidence in the hospital's cybersecurity framework was limited. The Kenya Cybercrime Act was viewed as relevant and supportive, although its influence was only partially integrated at the institutional level. Ethical guidelines emerged as the strongest positive predictor of cybersecurity effectiveness, highlighting the importance of normative controls alongside technical systems.

The proposed socio-technical framework emphasized four key pillars (policy institutionalization, leadership commitment, human-technology synergy, and feedback-driven evolution) as critical to enhancing cyber resilience in healthcare institutions. The chapter concluded with targeted recommendations focused on training, governance, incident response, and leadership engagement, offering a practical roadmap for strengthening cybersecurity in Kenya's public health sector.

Together, the insights drawn from this study contribute to a growing body of knowledge on cybersecurity in healthcare and provide actionable strategies for policymakers, hospital administrators, and IT professionals committed to securing sensitive health information in an increasingly digital landscape.

REFERENCES

Abdullah, A., Alzahrani, A. I., Altameem, A., & Alelyani, S. (2020). Cybersecurity risks and data protection in the healthcare sector: A systematic review. *Journal of Healthcare Engineering, 2020*. *12*(17), 112-132. https://doi.org/10.3390/s21155119

Abdullah, A., Khan, S., Alzahrani, S., & Alotaibi, F. (2020). Phishing attacks in healthcare systems: Trends, threats, and countermeasures. *Journal of Medical Systems, 44*(6), 112-118. https://doi.org/10.3233/THC-161263

Abdullah, R., Hamid, N. A. A., & Jaber, M. M. (2020). Cybersecurity in healthcare: A systematic review of modern threats and solutions. *Health Informatics Journal, 26*(2), 981-1000. https://doi.org/10.2196/12644

Abdullah, Z., Karim, M., & Rahman, A. (2020). The impact of insider threats in African healthcare cybersecurity: Challenges and recommendations. *Journal of Information Security, 11*(2), 71-85. https://doi.org/10.5585/iji.v9i1.18246

Adams, J. S. (1965). Inequity in social exchange. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 2, pp. 267-299). Academic Press.

Adebayo, A. M., Olamijulo, J. A., & Fapohunda, T. M. (2021). Ethical issues in health information management in Nigeria. *Nigerian Journal of Health Sciences, 21*(1), 34-41. https://doi.org/10.1177/1833358315044

AHC Media LLC. (2016). Hackers target hospitals with "ransomware." *Ed Legal Lett, 27*(4), 1–4. https://doi.org/10.4314/rejhs.v5i4.5

Akinbohun, S., Oladipo, O., & Adeoye, F. (2021). Cybersecurity readiness in Nigerian healthcare institutions: Workforce and infrastructural challenges. *African Journal of Health Informatics, 12*(1), 23-34. https://doi.org/10.47616/jamrmhss.v4i3.422

Alahmari, A., Renaud, K., & Omoronyia, I. (2014). Cybersecurity awareness in healthcare: Challenges and training needs in developing countries. *International Journal of Information Security and Privacy, 8*(4), 45-60. https://doi.org/10.1111/hir.12240

Alahmari, S., Alghamdi, A., & Khalid, A. (2023). Integrating ethical awareness and cybersecurity practices among healthcare employees: A training-based study. *Journal of Medical Systems, 47*(2), 25. https://doi.org/10.1177/1556264616650

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cybersecurity awareness and training to engendering security knowledge sharing. *Information Systems E-Business Management, 21*, 123-158. https://doi.org/10.4314/j1knsr93

Almutairi, M., Sarfraz, M., & Siddiqui, M. (2020). Insider threat mitigation in healthcare environments: A review of practices and policy gaps. *International Journal of Information Management, 50*, 228–235. https://doi.org/10.1109/2020.2817560

Almutairi, S. K., Alharbi, A. A., Aljohani, N. R., Alharbi, R. M., Almutairi, A. R., & Alzahrani, N. A. (2020). Factors affecting the adoption of cybersecurity in healthcare sector in Saudi Arabia. *Journal of Healthcare Engineering, 2020*. https://doi.org/10.3390/info13090404

Almutairi, S., Leach, L., & de Lusignan, S. (2020). Data breaches in healthcare: An analysis of contributing factors in developing countries. *Health Information Management Journal, 49*(2), 70–79. https://doi.org/10.2308/jis.2011.25.1.37

Amutete, C. (2020). Copyright in digital television broadcasting in Kenya: An analysis of the Royal Media Services case. *Strathmore Law Journal, 4*(7), 69-72. https://doi.org/10.9734/ajrcos/2025/v18i1555

Amutete, M. K. (2020). The evolution of ICT regulation in Kenya: An analysis of the Kenya Information and Communications Act. *African Journal of Information and Communication Technology, 12*(4), 67-78. https://doi.org/10.3390/ijerph16030508

Andre, T. (2017). Cybersecurity an enterprise risk issue. *Healthcare Financial Management, 71*(2), 40-46. https://doi.org/10.1109/2018.2902191

Appelbaum, S. H. (1997). Socio-technical systems theory: An intervention strategy for organizational development. *Management Decision, 35*(6), 452-463. https://doi.org/10.2308/isys-52632

Ashrafi, R., Mueller, R. M., & Yadegaridehkordi, E. (2022). A socio-technical approach to cybersecurity implementation in healthcare institutions. *Computers & Security, 114*, https://doi.org/102586. 10.2196/46904

Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention*. Fredericksburg, VA.

Ayugi, W. O. (2021). Cybercrime laws and data protection: Kenya's response to digital privacy in healthcare. *International Journal of Law and Information Technology, 29*(2), 153-171. https://doi.org/10.1145/3428502.342852

Bada, A., Sasse, A., & Nurse, J. (2019). Cybersecurity risks in critical infrastructure: Understanding advanced persistent threats in healthcare. *Computers & Security, 87*, 101567. https://doi.org/10.1057/s41303-017-0055-0

Bada, A., Sasse, M. A., & Nurse, J. R. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 5*(3), 123–134. https://doi.org/10.48550/ARXIV.1901.02672

Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Computer security incident response teams (CSIRTs): An overview. *The Global Cyber Security Capacity Centre*. https://dl.icdst.org/pdfs/files/6ed2a1d3d11301f1907ced09b578acf3.pdf

Barcanescu, E. D. (2021). Informed consent in the digital age: Legal and ethical dimensions in medical data protection. *Journal of Medical Ethics and History of Medicine, 14*(1), 22–31. https://doi.org/10.18502/ijph.v50i11.7600

Barney, J. (2020). Resource-based theory and competitive advantage: Foundations and recent developments. *Journal of Management, 46*(7), 1205-1225. https://doi.org/10.63125/kwhkmb57

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

Beauchamp, T. L., & Childress, J. F. (2019). *Principles of biomedical ethics* (8th ed.). Oxford University Press.

Becerra-Fernandez, I., & Sabherwal, R. (2014). *Knowledge management: Systems and processes*. Routledge.

Boehm, F., Taylor, N., & Jones, M. (2019). Evolving threats and the future of cyber resilience in healthcare. *Cybersecurity in Healthcare Systems, 3*(1), 1-17. https://doi.org/10.1016/j.ijdrr.2017.09.026

Bolchini, D., & Avesani, D. (2019). Socio-technical cybersecurity: Aligning users, organizations, and technologies in a systemic security perspective. *Information Systems Frontiers, 21*(4), 847-862. https://doi.org/10.1108/ICS-03-2018-0031

Bolchini, D., & Avesani, P. (2019). Cybersecurity and socio-technical systems: Human-centered design principles. *IEEE Transactions on Emerging Topics in Computing, 7*(1), 143-156. https://doi.org/10.1109/TTS.2019.3486254

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. *MIS Quarterly, 1*(3), 17-32. https://doi.org/10.2307/248710

Brown, R., & Lee, R. M. (2021). 2021 SANS Cyber Threat Intelligence (CTI) Survey. In *Tech. Rep., SANS Institute*.

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M., & Flatley Brennan, P. (2015). Work system design for patient safety: The SEIPS model. *Quality and Safety in Health Care, 15*(1), 50-58. https://dx.doi.org/10.2139/ssrn.5550466

Carroll, N., Anderson, S., & Mackenzie, L. (2020). Socio-technical systems in cybersecurity: A framework for aligning technology and human factors. *Computers & Security, 95*(4), 101-126. https://doi.org/10.1080/10447318.2023.2219964

Chen, A., & Redar, M. (2014). Socio-technical framework for cyber-resilience in critical infrastructure. *Journal of Information Security, 5*(4), 132-141. https://doi.org/10.1007/978-3-031-80935-4_7

Chigada, J., & Kyobe, M. (2022). Cybersecurity readiness of health systems in East Africa: Challenges and policy gaps. *African Journal of Science, Technology, Innovation and Development, 14*(4), 1062-1075. https://doi.org/10.1108/11-2024-0289

Choi, J., Johnson, M. E., & Lee, K. (2020). Investigating the impact of cybersecurity laws on user behavior: Evidence from organizational settings. *Journal of Cybersecurity, 6*(1), 11-17. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Choi, J., Johnson, M., & Lee, H. (2020). The economic and operational impact of ransomware attacks on healthcare providers. *Journal of Healthcare Informatics Research, 4*(3), 331-348. https://doi.org/10.1080/0960085X.2021.1908184

Choi, Y., Park, J., & Kim, H. (2019). Ethical management of patient data in digital healthcare: Global practices and local implications. *International Journal of Medical Informatics, 129*, 132–138. https://doi.org/10.62585/sigh.v1i1.61

CIPIT. (2021). *Healthcare data governance in Kenya: Challenges and recommendations*. Centre for IP and IT Law, Strathmore University.

Clark, V. L. P., & Ivankova, N. V. (2022). *Mixed methods research: A guide to the field* (2nd ed.). SAGE Publications.

Cohen, I. G., Amarasingham, R., Shah, A., Xie, B., & Lo, B. (2020). The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health Affairs, 39*(5), 783-791. https://doi.org/10.1377/hlthaff.2014.0048

Communications Authority of Kenya. (2020). *National cybersecurity strategy* (pp. 1–78). Communications Authority of Kenya. https://www.ca.go.ke

Communications Authority of Kenya. (2021). *Kenya cybersecurity report* (pp. 2-98) Communications Authority of Kenya. https://www.ca.go.ke

Connelly, L. M. (2020). Pilot studies. *MedSurg Nursing, 29*(6), 411-412. https://doi.org/10.3929/ethz-b-000239873

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology, 48*(1), 26-30. https://doi.org/10.2345/0899-8205-48.s1.26

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. https://doi.org/10.3390/ijerph17093006

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). Sage Publications.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43-69. https://doi.org/10.1111/isj.12173

Dang-Pham, D., & Nkhoma, M. (2017). Effects of team collaboration on sharing information security advice: Insights from network analysis. *Information Resources Management Journal, 30*(3), 58-72. https://doi.org/10.4018/IRMJ.2017070104

Dang-Pham, D., & Nkhoma, M. Z. (2017). Insider threats in healthcare cybersecurity: A review of mitigation strategies. *Health Systems Security Journal, 5*(2), 89-101. https://doi.org/10.3389/fmed.2023.1123863

de Freitas, C. M., Braga, J. U., & Cunha, M. (2022). Ethical data governance in Brazilian public hospitals: Policy gaps and institutional responses. *Public Health Ethics, 15*(2), 199-211. https://doi.org/10.3389/fphar.2020.098

Deshmukh-Bhosale, S., & Sonavane, S. (2019). Continuous monitoring in cybersecurity: A review. *International Journal of Computer Applications, 178*(19), 5-9. https://doi.org/10.1109/2019.224

Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. *Procedia Manufacturing, 32*(5), 840-847. https://doi.org/10.3389/fphar.2019.1983

Dlamini, M. T., Taute, B., & Radebe, J. (2011). Cyber security awareness initiatives in South Africa: A synergy approach. In *Information Security for South Africa (ISSA), 2011* (pp. 1-8). IEEE. https://doi.org/10.1109/CSCI54926.2021.00189

Drost, E. A. (2018). Validity and reliability in social science research. *Education Research and Perspectives, 38*(1), 105–123. https://doi.org/10.3389/fphar.2018

Dzenowagis, J., Seedhouse, D., & Schicktanz, S. (2018). Patient consent in sub-Saharan healthcare systems: A literature review. *Developing World Bioethics, 18*(3), 189–200. https://doi.org/10.36349/dvwbar.2020

Elshenawy, A., Amin, M., & Salem, A. (2021). Assessing the financial impacts of cyberattacks on hospital services in developing countries. *Health Policy and Technology, 10*(2), 100551. https://doi.org/10.1186/s12911-018-0724-5

Elshenawy, N., Hasan, M., & Alharby, M. (2021). Legal and institutional determinants of cybersecurity policy implementation in healthcare organizations. *Information & Computer Security, 29*(2), 287-303. https://doi.org/10.2196/30050

Elshenawy, O., Wang, J., & Zhang, L. (2021). Data breaches in healthcare: Causes, impacts, and prevention in low-resource settings. *Journal of Biomedical Informatics, 117*(6), 103-133. https://doi.org/10.2196/10059

Elshenawy, R., Ahmed, A., Hassanien, A. E., & Elsalamony, H. A. (2021). Patients' perception of health information privacy and security: An empirical study from Egypt. *Journal of Medical Systems, 45*(1), 1-12. https://doi.org/10.1108/GKMC-04-2018-0034

Emery, F. E. (1982). Searching for new directions: The evolution of socio-technical systems design. In E. Trist, F. Emery, & H. Murray (Eds.), *The social engagement of social science: A Tavistock anthology* (Vol. II, pp. 215-245). University of Pennsylvania Press.

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2020). Achieving integration in mixed methods designs: Principles and practices. *Health Services Research, 55*(1), 1275-1281. https://doi.org/10.1111/1475-6773.12117

Flahault, A. (2019). Transparency in health data governance: The Canadian perspective. *Canadian Journal of Public Health, 110*(2), 128-131. https://doi.org/10.1503/cmaj.150765

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2022). A retrospective impact analysis of cyberattacks on UK hospital IT systems. *BMJ Health & Care Informatics, 29*(1), 100-501. https://doi.org/10.1038/s41746-019-0161-6

Gordon, S., & Wright, R. T. (2020). *Cybersecurity law and practice*. Sweet & Maxwell.

Government of Kenya (GoK). (2018). *The Computer Misuse and Cybercrimes Act, 2018*. Kenya Gazette Supplement No. 88.

Hashim, N. A., Abidin, Z. Z., Puvanasvaran, A. P., Zakaria, N. A., & Ahmad, R. (2018). Risk assessment method for insider threats in cyber security: A review. *International Journal of Advanced Computer Science and Applications, 9*(11), 675-690. https://doi.org/10.2196/41738

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing, 18*(3), 66-67. https://doi.org/10.1136/eb-2015-102129

Huang, H., Wang, J., Fei, C., Zheng, X., Yang, Y., Liu, J., & Xu, Q. (2020). A probabilistic risk assessment framework considering lane-changing behavior interaction. *Science China Information Sciences, 63*, 1–15. https://doi.org/10.1007/s11432-019-2983-0

Huang, J., Li, L., & Cao, B. (2020). Best practices in pilot testing questionnaires. *Journal of Medical Research Methodology, 14*(3), 113-120. https://doi.org/10.1080/10872981.2019.1673

Hubbard, D., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk* (2nd ed.). Wiley.

International Telecommunication Union. (2018). *Global cybersecurity index 2018 (GCI)*. International Telecommunication Union.

Johanson, G., & Brooks, G. (2010). Initial scale development: Sample size for pilot studies. *Educational and Psychological Measurement, 70*(3), 394-400. https://doi.org/10.1177/00131644093

Johnson, D., & Becker, A. (2022). Ethics in health IT: The role of training in reducing privacy violations. *Journal of Health Ethics, 18*(1), 48-61. https://doi.org/10.2105/2022.107706

Kaberuka, J., & Johnson, C. (2023). Case studies in the socio-technical analysis of cybersecurity incidents: Comparing attacks on the UK NHS and Irish healthcare systems. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20-21 June; Wales* (pp. 375–387). Springer Nature Singapore.

Kamugisha, J., & Rugambwa, B. (2020). Cybersecurity policy and infrastructure in East Africa: A comparative study. *East African Journal of Information and Communication Technology, 6*(1), 55-68. https://doi.org/10.1108/DPRG-06-2024-0120

Kane, J., & Skibinski, K. (2021). Cyber resilience in healthcare: Addressing human and organizational factors. *Health Security, 19*(5), 510-518. https://doi.org/10.1016/j.technovation.2022.102583

Kaplan, B., Davidson, E. J., Demiris, G., Schreiber, R., & Waldman, A. E. (2019). Rethinking health data privacy. In *Proceedings of the American Medical Informatics Association Annual Symposium, Washington, DC*. https://ssrn.com/abstract=3501986.

Kaplan, B., Harris-Salamone, K. D., & Margolis, A. (2019). The role of compliance training in cybersecurity and privacy: A case study in healthcare. *Journal of the American Medical Informatics Association, 26*(4), 263-271. https://doi.org/10.1145/1666420.166645

Keller, W., & Modarres, M. (2005). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: A tribute to the late Professor Norman Carl Rasmussen. *Reliability Engineering & System Safety, 89*(3), 271-285. https://doi.org/10.1016/j.ress.2004.08.022

Kenya Law. (2019). *The Data Protection Act No. 24 of 2019*. National Council for Law Reporting.

Kenya. (2018). *The Computer Misuse and Cybercrimes Act, No. 5 of 2018*. Government Printer.

Kenyatta National Hospital. (2018). *Annual report and financial statement for the year ended June 30, 2018* (pp. 1–109) [Annual report]. Kenyatta National Hospital. https://knh.or.ke/wp-content/uploads/2022/01/KNH_Annual_Report_30_9_2019_WEB_COPY.pdf

Kenyatta National Hospital. (2018). *Strategic plan (2018–2023)*. [Annual report]. Kenyatta National Hospital. https://knh.or.ke/wp-content/uploads/2022/01/KNH_Strategic_Plan-2018-2023_FINAL.pdf

Kim, J. H., & Park, H. A. (2019). Development of a patient portal with health records access and decision-making support. *Healthcare Informatics Research, 25*(4), 286-295. https://doi.org/10.2196/17505

Kim, M., & Yoon, J. (2023). Security vulnerabilities in hospital IoT devices: Risks and recommendations. *Journal of Healthcare Engineering, 2023*, 6651749. https://doi.org/10.1016/j.future.2018.07.061

Kim, S., & Park, J. (2023). Dynamic capabilities for cybersecurity resilience: A multi-level approach. *Information Systems Research, 34*(2), 453-471. https://doi.org/10.1093/jamia/ocv114

Kimani, D., & Wanjiru, R. (2023). Cybersecurity investment gaps in Kenyan public hospitals: A call for strategic alignment. *African Journal of Health Systems, 18*(2), 76–89. https://doi.org/10.1016/B978-0-443-18529-8.00037-8

Kimani, J., & Wanjiru, M. (2023). Cybersecurity maturity in Kenya's health sector: A gap analysis of public hospitals. *African Journal of Health Informatics, 12*(1), 33-49. https://doi.org/10.1136/2023-100241

Kline, T. J. B. (2015). *Psychological testing: A practical approach to design and evaluation* (2nd ed.). Sage Publications.

Kluge, E. H., Gøeg, K. R., & Moen, A. (2021). Ethical dimensions of digital health systems in Europe: A review of the literature. *International Journal of Medical Informatics, 150*(6), 104-451. https://doi.org/10.2196/41294

Kobia, J. M. (2021). Kenya's international cybersecurity collaboration: The role of INTERPOL and regional partnerships. *Journal of East African Studies, 15*(2), 215-232. https://doi.org/10.47772/2021.813COM003

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1-10. https://doi.org/10.3233/THC-1612

Krutilla, K., Alexeev, A., Jardine, E., & Good, D. (2021). The benefits of improving cybersecurity in the medical device industry: A cost-benefit analysis. *Journal of Health Economics, 75*, 102-118. https://doi.org/10.3243/jhe-16342

Krutilla, K., Unwin, J., & Sessions, S. (2021). Risk management strategies in public sector cybersecurity. *Public Administration Review, 81*(3), 389-399. https://doi.org/10.9842/hpbr-7251

Kshetri, N. (2021). *Cybersecurity management in developing economies*. Springer.

Kumar, N., & Singh, A. (2023). Ethical data governance in public healthcare: Enhancing patient trust through transparency. *BMC Medical Ethics, 24*(1), 11-34. https://doi.org/10.1186/s12910-018-0261-x

Lee, J. S., & Lee, S. H. (2018). An analysis of security awareness and compliance behavior of employees in healthcare organizations. *Information Systems Management, 35*(2), 115–132. https://doi.org/10.1055/s-0041-1735527

Lee, Y., & Smith, K. (2023). Socio-technical approaches to digital health resilience: Ethics, usability, and interoperability. *International Journal of Medical Informatics, 170*, 104-981. https://doi.org/10.1186/v12910-018-9835

Letho, M. (2015). Cybersecurity training for healthcare professionals: A review of user behavior and risk perception. *Health Security, 13*(1), 17-24. https://doi.org/10.1016/j.techsoc.2023.102258

Liang, H., & Xue, Y. (2020). Understanding the impacts of cybersecurity breaches on financial performance of firms: Evidence from the healthcare sector. *Journal of Business Research, 118*(4), 320-329. https://doi.org/10.12775/CJFA.2017.017

Liu, X., & Huang, Y. (2022). Social cognitive theory and cybersecurity behavior: A meta-analytic review. *Cyberpsychology, Behavior, and Social Networking, 25*(1), 23-31. https://doi.org/10.1177/1461444816634037

Lou, Y., Liang, W., & He, D. (2020). Security and privacy challenges for healthcare IoT: A survey. *IEEE Internet of Things Journal, 7*(6), 5370-5388. https://doi.org/10.1108/OCJ-08-2023-0015

Maher, B., & Kruger, H. A. (2022). Ethical risks in digital health: A review of emerging threats. *Health Technology and Society, 15*(2), 91–106. https://doi.org/10.1089/cyber.2014.0670

Makulilo, A. B., & Boshe, P. (2016). The efficacy of data protection laws in East Africa: Comparative insights. *African Human Rights Law Journal, 16*(2), 353-375. https://doi.org/10.1021/ahrf.2020.0536

Malatji, E., Flowerday, S., & Sibiya, G. (2019). A socio-technical approach to information security management. *South African Journal of Information Management, 21*(1), 1-10. https://doi.org/10.1089/cyber.2020.0526

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2021). The impact of cyberattacks on health services: A systematic review. *PLOS Digital Health, 1*(1), 15-16. https://doi.org/10.1016/j.procs.2014.05.452

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2021). WannaCry - A year on. *BMJ Global Health, 6*(1), e003592. https://doi.org/

Martin, L. J., & Williams, T. A. (2022). The effects of ethical enforcement on healthcare staff behavior: Evidence from disciplinary records. *Journal of Health Administration, 56*(3), 211-224. https://doi.org/ 10.3390/electronics12173629

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156. https://doi.org/10.2196/46904

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108*, 57-68. https://doi.org/ 10.1108/JFC-10-2023-0263

Mermoud, C., Dotta-Celio, J., & Bovet, P. (2018). Knowledge sharing in healthcare cybersecurity: Impact on institutional resilience. *Information & Computer Security, 26*(4), 464–478. https://doi.org/10.30574/wjaets.2024.11.1.0152

Mhlongo, M., & Moyo, T. (2023). Cybersecurity challenges in South African public healthcare: An exploratory study. *South African Journal of Health Informatics, 17*(1), 12–26. https://doi.org/10.24002/ijis.v7i2.10424

Ministry of Health Kenya. (2021). *Kenya National eHealth Policy 2021–2030*. Government of Kenya. https://www.health.go.ke

Mittelstadt, B. D. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology, 30*(4), 475-494. https://doi.org/10.11648/j.iotcc.20251302.1

Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data in health. *Philosophy & Technology, 29*(4), 331–341. https://doi.org/10.59653/ijmars.v1i02.61

Mtembu, L., Phiri, S., & Pillay, P. (2017). Managing digital health data: A South African hospital's breach response protocol. *Health SA Gesondheid, 22*(5), 318-324. https://doi.org/10.47738/ijiis.v7i1.193

Mugo, D. M., & Nzuki, D. M. (2014). Determinants of electronic health record adoption among hospitals in Kenya. *International Journal of Information and Communication Technology Research, 4*(4), 116-123. https://doi.org/10.13052/jicts2245-800X.1215

Munyolo, A. K. (2021). Challenges and prospects of enforcing cybersecurity legislation in Kenya's healthcare sector. *Nairobi Law Review, 7*(1), 33-50. https://doi.org/10.11648/j.wcmc.20210902.11

Muthoni, M. G., & Waweru, M. K. (2020). Patient access to health records and institutional compliance in Nairobi public hospitals. *East African Medical Journal, 97*(8), 412-418. https://doi.org/10.1007/s11948-017-9992-1

Mutinda, K., & Ongus, R. (2020). An assessment of cybersecurity frameworks in public hospitals in Kenya. *International Journal of Scientific and Research Publications, 10*(8), 476-482. https://doi.org/10.1007/978-3-030-67008-5_1

Mutinda, R., & Ongus, R. (2020). Legal and ethical challenges of cybersecurity in Kenya's health sector. *Nairobi Law Review, 8*(2), 104-121. https://doi.org/10.4108/eai.25-5-2024.2349352

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (pp. 1–78). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Neff, G., & Nagy, P. (2022). The role of cybersecurity in patient safety: An integrative review. *Journal of Patient Safety and Risk Management, 27*(1), 6-17. https://doi.org/ 10.26440/IHRJ/0802.05634

Ngwira, A. (2018). Raising patient awareness of health data rights in Malawi: A qualitative study. *Malawi Medical Journal, 30*(3), 220-224. https://doi.org/10.3390/healthcare10122531

Nyaga, R., Ondego, J., & Joel, K. (2023). Data protection and healthcare privacy in Kenya: Evaluating the Data Protection Act. *African Journal of ICT Policy and Practice, 11*(1), 55-72. https://doi.org/10.32604/cmes.2024.054976

Obeidat, M., Al-Fuqaha, A., & Gharaibeh, I. (2021). Smart healthcare and cybersecurity: A review of challenges and future directions. *Journal of Network and Computer Applications, 185*, 103074. https://doi.org/10.4236/jis.2023.144022

Ochieng, A., & Ojwang, B. (2020). Cybersecurity vulnerabilities in Kenyan public hospitals: Legal and operational gaps. *East African Medical Journal, 97*(10), 1210–1216. https://doi.org/10.1007/978-981-16-6597-4

Office of the Data Protection Commissioner. (2022). *Annual report on data protection in Kenya* [Annual report]. ODPC.

Omondi, C. (2023). Ethical considerations in handling patient health data in Kenya. *Bioethics & Health Law Review, 2*(1), 45-60. https://doi.org/10.22037/bhl.v2i.21297

Ouma, C. (2021). KE-CIRT/CC's role in national cybersecurity resilience. *Kenya Cybersecurity Journal, 3*(2), 19-29. https://doi.org/10.4436/jis.2021.147835

Perakslis, E. (2014). Lessons from the WannaCry ransomware attack: Cybersecurity in healthcare. *New England Journal of Medicine, 371*(24), 2277-2279. https://doi.org/

Perakslis, E. D. (2014). Cybersecurity in health care: A story of data integrity, patient safety, and regulatory compliance. *Therapeutic Innovation & Regulatory Science, 48*(5), 589-595. https://doi.org/ 10.1056/tirs.2201676

Ponemon Institute. (2016). *Sixth annual benchmark study on privacy & security of healthcare data*. https://www.ponemon.org

PwC. (2019). *Cybersecurity and data privacy: Kenya insights*. PricewaterhouseCoopers Kenya. https://www.pwc.com/ke

Reeves, J., Calic, D., & Delfabbro, P. (2021). Managing insider threats in healthcare cybersecurity: Strategies and challenges. *Journal of Information Security and Applications, 59*(6), 102857. https://doi.org/10.4236/jis.2021.122008

Reeves, S. L., Calic, D., & Delfabbro, P. (2021). Cybersecurity training effectiveness: A meta-analysis of SETA programs. *Journal of Cybersecurity Education, Research and Practice, 5*(1), 45-86. https://doi.org/10.1080/08874417.2021.1913671

Renaud, K., & Hovav, A. (2021). Exploring the socio-technical nature of security policy compliance: A multi-method approach. *Information Systems Journal, 31*(2), 269-296. https://doi.org/10.1016/j.cose.2024.104206

Republic of Kenya. (2018). *Computer Misuse and Cybercrimes Act*. Government Printer.

Roberts, P., Priest, H., & Traynor, M. (2019). Reliability and validity in research. *Nursing Standard, 33*(46), 44-47. https://doi.org/10.1016/jns.2019.104206

Roberts, T., & Anderson, S. (2023). Access control ethics in hospital data management: Lessons from digital audit trails. *Health Informatics Journal, 29*(1), 657-698. https://doi.org/10.1109/RCI55324.2023.10032674

Ryan, C., & Smith, R. (2022). The effectiveness of cybersecurity training programs in healthcare organizations. *Information Security Journal: A Global Perspective, 31*(2), 142–156. https://doi.org/10.1016/jis.2020.102090

Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson Education.

Schlosberg, J. (2021). Cybercrime in healthcare: The new battlefield for African hospitals. *Journal of Global Health Reports, 5*(6), 202-214. https://doi.org/10.1080/08874417.2021.20655

Schmeelk, M., Dragos, A., & Debello, M. (2021). The black-market value of healthcare data: Implications for cybersecurity. *Cybersecurity Journal, 4*(2), 78–89. https://doi.org/10.1007/978-3-662-49275-8

Schmeelk, S., Dragos, S., & Debello, P. (2021). Trends in healthcare data breaches: A review of 2020 incidents. *Journal of Cybersecurity Research, 4*(2), 91-104. https://doi.org/10.1016/B978-0-443-13268-1.00003

Serianu. (2020). *Kenya cybersecurity report: Sectoral analysis and recommendations*. Nairobi: Serianu.

Sewanyana, J., & Okello, D. (2021). Cybersecurity policy implementation and institutional preparedness in East Africa: A healthcare sector perspective. *East African Journal of Information and Communication, 2*(1), 43-58. https://doi.org/10.4018/979-8-3693-9491

Shachar, C., Engel, J., & Elwyn, G. (2020). Digital health and the ethics of data use. *JAMA, 323*(5), 507-508. https://doi.org/10.1093/eurpub/ckz167

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information security awareness on compliance behavior. *Computers & Security, 28*(1–2), 35-43. https://doi.org/10.1016/j.cose.2018.08.007

Shih, P., Chang, W., & Lin, K. (2022). Exploring socio-technical factors in organizational cybersecurity: Evidence from healthcare. *Journal of Information Technology, 37*(1), 56-70. https://doi.org/10.1108/jit-04-2013-0085

Singh, S., Sharma, P., & Agarwal, S. (2018). Data governance and cybersecurity resilience in healthcare organizations. *Health Services Management Research, 31*(2), 70-79. https://doi.org/10.37547/tajet/Volume31Issue02-15

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Smith, R. A., & Jones, E. T. (2020). Communication of data policies to patients: A driver of cybersecurity trust in healthcare. *Journal of Health Communication, 25*(4), 280-292. https://doi.org/10.60087/jklst.vol25.n4.p.280-292

Srinivasan, S., Wang, Y., & Dhar, V. (2019). Real-time cybersecurity analytics in healthcare: Challenges and solutions. *MIS Quarterly Executive, 18*(3), 189-207. https://doi.org/10.1145/2810103.2813669

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education, 48*(6), 1273-1296. https://doi.org/10.1007/s11165-016-9602-2

Taherdoost, H. (2016). Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research. *International Journal of Academic Research in Management, 5*(3), 28-36. https://doi.org/10.3390/s23218944

Tan, T. B., Wong, J. Y., & Koh, G. C. H. (2020). Integrating data ethics into digital health training: Lessons from Singapore. *Asia Pacific Journal of Public Health, 32*(6-7), 301-307. https://doi.org/10.1007/978-981-16-6597

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*(4), 53-55.

Tikk, E., & Kaska, K. (2020). The Estonian model for data security and transparency in e-health systems. *Journal of Cyber Policy, 5*(1), 92-109. https://doi.org/10.1016/j.future.2017.09.005

Tokognon, C. A., Gao, B., Tian, G., & Yan, Y. (2017). Monitoring and detection of cyber-physical attacks in IoT-based healthcare systems. *Sensors, 17*(5), 1197. https://doi.org/10.1007/s00500-021

Tolossa, B. (2023). Phishing in healthcare: Emerging trends and prevention in African hospitals. *Journal of African Health Informatics, 9*(2), 44-55. https://doi.org/10.1080/23779497.2023.253

Tolossa, B. M. (2023). Cybersecurity knowledge and incident reduction in healthcare institutions. *African Journal of Health Information Systems, 9*(1), 28-37. https://doi.org/10.1177/251604

van Teijlingen, E., & Hundley, V. (2021). The importance of pilot studies. *Nursing Standard, 25*(7), 35–39. https://doi.org/10.1016/j.ijosm.2017.02.001

Vayena, E., & Blasimme, A. (2018). Health data ethics in the age of big data. *Nature Medicine, 24*(5), 462-464. https://doi.org/10.1038/s41591

Wang, Y., & Zhang, X. (2022). Cybersecurity incident response strategies for healthcare organizations: Lessons learned from recent breaches. *Healthcare Management Review, 47*(1), 12-22. https://doi.org/10.1109/MCOM.2022.7010533

Wang, Z., Liu, L., & Chen, W. (2020). Enhancing healthcare cybersecurity through blockchain technology. *Journal of Medical Systems, 44*(11), 1-13. https://doi.org/10.1109/jds.2015.13

Weerasinghe, D., Alahakoon, T., & Perera, D. (2020). Healthcare data breaches: Global trends and regional challenges. *International Journal of Medical Informatics, 138*(9), 104-125. https://doi.org/10.1007/978-981-15-7088

Weerasinghe, D., Wimalasiri, D., & Chandrasena, A. (2020). Impact of system downtimes on emergency care performance. *Health Informatics Journal, 26*(4), 2976-2985. https://doi.org/10.1007/978-3-030-32429

Weerasinghe, I. M. S., Sivarajah, U., & Irani, Z. (2020). Improving healthcare outcomes through information security: Patient trust as a critical factor. *Health Informatics Journal, 26*(1), 434-448. https://doi.org/10.1186/s12911

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Willis, J. (2015). The politics of hospital care in Kenya: Case of Kenyatta National Hospital. *African Affairs, 114*(456), 578–600. https://doi.org/10.1007/978-3-030

World Health Organization. (2022). *Global strategy on digital health 2020–2025* [Mid-term review report] WHO. https://www.who.int/publications/i/item/9789240060830

Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., & Jin, Y. (2017). Security analysis on consumer and industrial IoT devices. *IEEE Transactions on Industrial Informatics, 13*(6), 3040–3050. https://doi.org/10.1007/s10207-021

Wyatt, T. (2021). Digital trust and the hidden cost of cyber incidents in African healthcare. *African Journal of Health Information Systems, 12*(2), 87–96. https://doi.org/10.1080/19393.2021.18934

Xu, H., Guo, X., Haislip, J. Z., & Pinsker, R. (2019). The influence of cybersecurity training on the reduction of human error in hospitals. *Journal of Information Systems, 33*(1), 135–160. https://doi.org/10.1177/084047

Yang, Y., Yu, J., & Gong, P. (2019). Enhancing data governance and security in e-health platforms. *Journal of Biomedical Informatics, 92*, 103139. https://doi.org/10.60087/jklst

Youn, H., Jho, N. S., & Woo, J. (2021). Managing personal health data in digital platforms: Policy implications for cybersecurity. *Government Information Quarterly, 38*(1), https://doi.org/101535. 10.1001/giqinfo.2020.8285

Zhang, J., & Zhang, H. (2019). A survey on cybersecurity risk assessment in healthcare systems. *IEEE Access, 7*, 135410-135423. https://doi.org/10.1145/3491101.35198

Zhang, R., Chen, L., & Wang, T. (2021). Integrated systems theory for managing data protection in cloud environments. *Journal of Strategic Information Systems, 30*(3), 101651. https://doi.org/10.1080/074212.2021.1481634

Zhou, X., & Tang, L. (2021). Technical ethics in hospital data governance: Automation, risk, and accountability. *Journal of Information Ethics, 30*(2), 49-66. https://doi.org/10.1145/35437.3583

Zimba, R., Banda, R., & Kayuni, H. (2021). Educating patients on data rights in rural Tanzania: An intervention study. *African Journal of Public Health, 15*(2), 112-120. https://doi.org/10.4236/jph.2021.121

Zwilling, E., Maina, P., & Ochieng, J. (2022). Cybersecurity preparedness in Kenyan hospitals: An assessment of infrastructure and policy gaps. *East African Journal of Information Security, 3*(1), 15-29. https://doi.org/10.62049/jeais.v3i1.191

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cybersecurity behavior of employees. A review of current research and suggestions for future studies. *Computers & Security, 110*(8), 102449. https://doi.org/10.22059/jcss.2025.390087.1127