

**A WEB-BASED MODEL TO DETERMINE CYBERSECURITY READINESS
INDEX FOR HOSPITALS TOWARDS ADOPTION OF E-HEALTH**

AIYABEI EDWIN KIPLIMO

**A Research Thesis submitted to the Institute of Postgraduate Studies in
Partial fulfilment for the award of Master of Science in Information
Technology of Kabarak University.**

KABARAK UNIVERSITY

SEPT, 2018

DECLARATION

I, Aiyabei Edwin Kiplimo, do hereby declare that this thesis is my original work and where there's contribution of other individuals, it has been dully acknowledged.

Signature Date

Aiyabei Edwin Kiplimo

GMI/NE/0846/05/16

RECOMMENDATION

This thesis is the candidate's original work and has been prepared with my guidance; it has been submitted with my approval as the official university supervisor.

Signature..... Date.....

Prof. Kefa Rabah

Department of Computer Science,
Kabarak University.

Signature.....Date.....

Prof. Simon Maina Karume

Department of Computing and informatics,
Laikipia University.

COPYRIGHT

© 2018 Aiyabei Edwin

All rights Reserved

This thesis is protected by Copyright laws and therefore no part of this thesis may be distributed or reproduced without the consent of the author or that of Kabarak University.

DEDICATION

I dedicate this study to my parents Mr and Mrs Alex and Jackline Kimeli, my siblings;
Amos, Judy, Cynthia, Brian and Emmaculate.

ACKNOWLEDGEMENTS

First, I wish to express my sincere gratitude to my supervisors Prof. Kefa Rabah and Prof. Simon Karume for their professional advice and help throughout this research thesis. Secondly, my sincere thanks goes to my classmates for their support throughout the study and also my parents for their continued support both financially and spiritually which made this study a success. Above all my heartfelt gratitude goes to the almighty God for the provision of wisdom and wellbeing.

ABSTRACT

The main goal of healthcare sector worldwide is to provide quality and efficient health services to citizens. As the threat landscape on healthcare continues to escalate, many hospitals still lag behind in terms of protecting its critical infrastructure and electronic protected health information (ePHI). This research provided solution by designing a web application that will help the healthcare determine its Cybersecurity Readiness Index (CRI). The research targeted 55 respondents from 11 hospitals both private and public operating within Nakuru County. 50 questionnaires were returned translating to 91% response rate. The design of the model was based on 4 cybersecurity elements (people, process, policy, and technology). After an in depth analysis it was established that there existed a positive and statistically significant correlation between CRI and each of the four cybersecurity elements. Relevant weights for designing the mathematical model were derived using regression analysis. The model was implemented as a web based application through design science using PHP as a server-side language, MYSQL as a database engine and Bootstrap for the responsive front-end. This research is significant in the sense that, hospitals will be able to check their cyber readiness status, maintain its systems, sustain its operations, protect against current and future cyber threats, and respond and recover from it.

Key words: web application, cyber-attack, cyber readiness, people, process, technology, policy.

TABLE OF CONTENT

DECLARATION	ii
RECOMMENDATION	iii
COPYRIGHT	iv
DEDICATION	v
ACKNOWLEDGEMENTS	vi
ABSTRACT	vii
LIST OF TABLES	xi
LIST OF EQUATIONS	xii
LIST OF FIGURES	xiii
ABBREVIATIONS	xiv
OPERATIONAL DEFINITIONS OF TERMS	xv
CHAPTER ONE:INTRODUCTION	1
1.1 Introduction	1
1.2 Background to the Study	1
1.3 The Statement of the Problem	3
1.4 Purpose of the Study	4
1.5 Objectives of the Research	4
1.6 Research Questions	4
1.7 Significance of the Research	5
1.8 Expected Outcome for the Study	5
1.9 Justification for the Study	5
1.10 Scope of the Study.....	6
1.11 Limitations of the Study	6
1.12 Scalability	6
CHAPTER TWO:LITERATURE REVIEW	7
2.1 Introduction	7
2.2 What needs to be Protected?	7
2.3 People	8
2.3.1 Awareness and Training	9
2.3.2 Importance of Security Awareness and Training	10
2.3.3 Human Resources Security (ISO).....	12
2.4 Process.....	13
2.4.1 Awareness Process	14
2.4.2 Access Process.....	15
2.4.3 Compliance Process.....	18
2.4.4 Capability Maturity Model (CMM).....	19
2.5 Technology	21
2.5.1 Network Security	21
2.5.2 Managing User Privileges	27
2.5.3 Removable Media Control.....	28
2.5.4 Malware Protection.....	28
2.5.5 Secure Configuration	29
2.6 Policy.....	30
2.6.1 Security policy components.....	30
2.6.2 Acceptable Use Policy	31
2.6.3 Encryption Policy	32
2.6.4 Information Security Policy.....	32
2.6.5 Wireless Use Policy	32
2.6.6 Backup Policy.....	33
2.7 Models Informing the Study	33

2.7.1 Cyber Readiness Index 2.0	33
2.7.2 Cybersecurity Self-Assessment Tool.....	33
2.7.3 SSH Hong Kong Enterprise Cyber Security Readiness Index	34
2.7.4 Global Cybersecurity Index (GCI)	35
2.7.5 ISO/IEC 27001	36
2.7.6 The Health Insurance Portability and Accountability Act (HIPAA).....	38
2.7.7 Health Information Trust Alliance (HITRUST).....	38
2.7.8 Common Security Framework (CSF).....	38
2.8 Research Gap.....	39
2.9 Conceptual Framework	39
CHAPTER THREE:RESEARCH DESIGN AND METHODOLOGY.....	42
3.1 Introduction	42
3.2 Research Design.....	42
3.3 Location of the Study	42
3.4 Population of the Study	43
3.5 Sampling Procedure and Sample Size.....	43
3.6 Instrumentation.....	43
3.6.1 Validity of the Instrument.....	43
3.6.2 Reliability of the Instrument.....	44
3.7 Data Collection Procedure	44
3.8 Model Development.....	44
3.9 Model Implementation	45
3.10 Prototype Evaluation	45
3.11 Ethical Considerations.....	46
CHAPTER FOUR:DATA ANALYSIS, PRESENTATION AND DISCUSSION	47
4.1 Introduction	47
4.2 Response Rate	47
4.3 General Information	47
4.3.1 Hospital Category	47
4.3.2 Position	47
4.4 Assessment of Cyber Security Readiness Elements	48
4.4.1 Cybersecurity elements Criticality	48
4.4.2 Descriptive Findings.....	48
4.5 Cyber Security Readiness Model design.....	55
4.5.1 Correlation between System User’s Awareness against Cyber Security Readiness	56
4.5.2 Correlation between the Laid Down Procedures of Operation for Monitoring Cybersecurity against the Cyber Security Readiness	56
4.5.3 Correlation between the Adoption of Cyber Security Policy and Cyber Security Readiness.....	56
4.5.4 Correlations between IT Safeguards and Cyber Security Readiness	56
4.6 Regression Analysis	57
4.6.1 Model Summary	57
4.6.2 Anova Statistics	57
4.6.3 Regression Coefficients.....	58
4.7 Derivation of Relevant Weight for CRI Mathematical Model.....	58
4.8 Model Scenarios.....	59
4.8.1 Best Case Scenario	59
4.8.2 Average Case Scenario	59
4.8.3 Worst Case Scenario.....	59

4.9 Threshold Scores and assessment scale	60
4.10 Model Implementation	61
4.10.1 CRI System Design	61
4.10.2 System Objective	61
4.10.3 System Function Overview	61
4.10.4 Processes to Complete SREI System functionality	62
4.10.4 CRI System Architecture	63
4.10.6 System Design	64
4.10.7 System evaluation	74
4.10.8 Validation Process	77
4.10.9 Model Case Scenario Evaluation	77
CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS	79
5.1 Introduction	79
5.2 Summary	79
5.3.1 Objectives Address	80
5.3.2 Recommendations	81
5.3.3 Recommendation for further research.	82
REFERENCES.....	83
Appendix I: Hospitals selected for the Research	89
Appendix II: Questionnaire.....	90
Appendix III: NACOSTI Research Authorization.....	95
Appendix IV: Ministry of Education Research Authorization	96
Appendix V: Ministry of Interior and Co-ordination on National Government Research Authorization	97
Appendix VI: NACOSTI Research Clearance Permit	98
Appendix VII: Publication.....	99
Appendix VIII: System Code.....	100

LIST OF TABLES

TABLE 2.1: SSH HONG KONG ENTERPRISE CYBER SECURITY READINESS INDEX	35
TABLE 4.1: HOSPITAL CATEGORY.....	47
TABLE 4.2: POSITION HELD	47
TABLE 4.3: CYBERSECURITY ELEMENTS CRITICALITY	48
TABLE 4.4: SYSTEM USER'S AWARENESS WITH REGARD TO CYBER SECURITY.....	49
TABLE 4.5: PROCEDURES OF OPERATION FOR MONITORING CYBERSECURITY.....	51
TABLE 4.6: ADOPTION OF CYBER SECURITY POLICY	52
TABLE 4.7: SAFEGUARD OF IT SYSTEMS AGAINST CYBER ATTACKS.....	54
TABLE 4.8: SPEARMAN'S RHO CORRELATIONS	55
TABLE 4.9: IT SYSTEM AS SUCH' GOAL BASED EVALUATION.....	75
TABLE 4.10: HEURISTIC EVALUATION	76

LIST OF EQUATIONS

EQUATION 1: MODEL EQUATION	44
EQUATION 2: MULTIPLE REGRESSION	58
EQUATION 3: BEST CASE SCENARIO	59
EQUATION 4: AVERAGE CASE SCENARIO.....	59
EQUATION 5: WORST CASE SCENARIO.....	60

LIST OF FIGURES

FIGURE 1: HEALTHCARE ATTACK SURFACE.....	7
FIGURE 2: AWARENESS PROCESS	15
FIGURE 3: SIMPLE PACKET FILTER.....	22
FIGURE 4: APPLICATION LEVEL GATEWAY	23
FIGURE 5: CIRCUIT LEVEL GATEWAY	24
FIGURE 6: ACCESS CONTROL PROCESS	25
FIGURE 7: ROLE OF IPS AND IDS IN NETWORK SECURITY	27
FIGURE 8: NETWORK SECURITY CONCEPTS AND POLICIES	30
FIGURE 9: PILLARS OF GCI.....	36
FIGURE 10: PDCA MODEL	37
FIGURE 11: CONCEPTUAL FRAMEWORK	40
FIGURE 12: ARCHITECTURAL CONCEPTUAL FRAMEWORK.....	41
FIGURE 13: RAPID PROTOTYPE MODEL.....	45
FIGURE 14: ASSESSMENT SCALE.....	60
FIGURE 15: CRI SYSTEM FLOW CHART.....	62
FIGURE 16: ENTITY RELATIONSHIP DIAGRAM	63
FIGURE 17: CRI SYSTEM NAVIGATION PANEL	65
FIGURE 18: REGISTRATION PROCESS FLOWCHART	66
FIGURE 19: REGISTRATION GUI	67
FIGURE 20: LOGIN PROCESS FLOWCHART.....	68
FIGURE 21: LOGIN GUI.....	68
FIGURE 22: READINESS ASSESSMENT FLOWCHART	69
FIGURE 23: RISK ASSESSMENT GUI.....	70
FIGURE 24: SCORE FLOWCHART	71
FIGURE 25: SCORES GUI.....	71
FIGURE 26: RECOMMENDATIONS FLOWCHART	72
FIGURE 27: RECOMMENDATION GUI	73
FIGURE 28: HELP GUI.....	73
FIGURE 29: HOME GUI	74
FIGURE 30: MODEL VERIFICATION AND VALIDATION.....	77
FIGURE 31: WORST CASE SCENARIO GUI.....	77
FIGURE 32: AVERAGE CASE SCENARIO GUI.....	78
FIGURE 33: BEST CASE SCENARIO GUI	78

ABBREVIATIONS

AAA	Authentication, Authorization Accounting
BYOD	Bring Your Own Device
CMM	Capability Maturity Model
EMR	Electronic Medical Records
ePHI	Electronic Protected Health Information
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability
ICT	Information and Communication Technology Act
ICU	Intensive Care Unit
IEC	International Electro technical Commission
ISMS	Information Security Management System
IoT	Internet of Things
ISO	International Organization for Standardization
OWASP	Open Web Application Security Project
PHI	Protected Health Information
UHC	Universal Health Coverage
USB	Universal Serial Bus
SD	Secure Digital

OPERATIONAL DEFINITIONS OF TERMS

Model	A representation that can be graphical, mathematical, physical or verbal that provides a simplified version of a phenomena, structure, system, concept, or relationship of things in the real world. (Farlex, 2009)
People	Human beings making up a group or assembly or linked by a common interest (Merriam-Webster,n.d). Used in this research to mean System Users
Policy	A deliberate system of principles to guide decisions and achieve rational outcomes (Wikipedia, n.d.). Used in this research to refer to Laid Down Procedures of Operation for Monitoring Cybersecurity
Process	Series of actions directed to some end (Kuhlthau, 2004). Used in this research to mean series of actions or steps taken to achieve Cybersecurity
Security threat	Refers to anything that has a possibility of causing harm to information or information system (Techopedia, 2016).
Technology	Any electronic item/application/equipment or virtual network that is used with the intention to increase/maintain, and/or improve daily living and productivity (Wong et al., 2015). Used in this research to mean any electronic item put in place to achieve Cybersecurity
Web application	Program that is accessed over a network connection, rather than existing within a device's memory. (Techopedia, 2016). Used in the study to mean CRI model

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This Chapter presents the background and the purpose of the study. It presents the statement of the problem, the study objectives, and the research questions. This chapter also introduces the significance of the study, expected outcomes, justification, scope, limitations, and the scalability of the study.

1.2 Background to the Study

The proliferation of information communication technology (ICT) among organizations is a force to reckon with in this digital revolution age. The past decade has seen tremendous uptake of ICT worldwide (Luo & Bu, 2016). The adoption of ICT among organizations provides a competitive advantage for organizations that have adopted it over the ones that have not. Healthcare sector is an example institutions that have embraced information technology in an effort to provide efficient and quality healthcare services to citizens as well as providing universal health coverage (UHC). Healthcare sector is an information intensive, service and process oriented thus requiring a suitable technological advances in facilitating efficiency, reliability and effectiveness (Gambo & Soriyan, 2017). ICT plays a critical role in hospitals ranging from management of electronic medical records (EMR) to application in vital settings such intensive care unit (ICU). Cyber-attack has become more severe in large healthcare organizations such as hospitals due to the shift from stand-alone applications to tightly integrated applications that are attached to networks. These networks integrates variety of departments such as pharmacy, radiology, billing and clinical laboratory (Harries & Yellowlees, 2013). These networks are also connected to external networks for the purpose of connecting and sharing information with suppliers, insurers and employees. When systems with such large attack surface is compromised then the effect is catastrophic.

As networked medical devices becomes more embedded in healthcare, the attack surface is also increased. The increased reliance of digital applications and cyberspace has not only brought numerous benefits but also exposed the healthcare to a lot of cyber threats. These cyber issues range from malware that compromises with the integrity of healthcare systems and privacy of patients to denial of service (DoS) that disrupts the provision of services. Whatever shape the attack takes, the overall

consequences are the same; patients care is at stake and the trust in the healthcare system goes down (Harries & Yellowlees, 2013).

In recent report on attack on healthcare, a whopping 94% of healthcare institutions have been victims of cyber-attack (Perakslis, 2014). The increased number of attacks in healthcare sector is attributed to a combination of two factors: on one hand, the high value of healthcare assets it possesses and on the other hand, the ease at which these facilities can be compromised. According to KPMG (2015), healthcare industry is by far as compared to other industries such as financial sectors in protecting its infrastructure. This makes healthcare more vulnerable to attack as attackers get high rewards at low cost. Another reason that makes healthcare sector more lucrative to hackers is the sensitive data it possess. For example the protected health information (PHI) contains sensitive patient's information such as account number, health insurance numbers, medical record numbers and other important information as outlined by insurance portability and accountability act (HIPAA). Such information may be used for medical identity theft (Andrews, 2016). Over the past few decades, attack on financial sector has been the talk of the town due to financial motivation but lately there has been a shift. In 2016 for example the number of attacks reported on banks was less compared to reported attacks to healthcare. Threats to medical devices and vital healthcare infrastructure is critical since it has potential effects to patient's safety and health.

According Independent Security Evaluator (2016) cyber security laxity in healthcare can be attributed to three levels; organizational, physical and technical level. At the organizational level the main issue is lack of funding to information security. The funding being allocated to information security is so minimal that it cannot allow for defence in depth of healthcare infrastructure. This small allocation of funds is attributed to lack of awareness in ensuring patient's safety. The technical level issue is attributed to lack of appropriate expertise from the information technology technical team. This inevitably causes security attacks and vulnerabilities as a result of misconfiguration of systems, delays in upgrading and updating systems. The physical level is not directly linked to cyber threats but it plays a big role in safeguarding healthcare systems. This involves physical access to hospital network that exposes the hospital to attack.

In response to an increase in volume and sophistication of cyber threats, health care sector is encouraged to assess its cybersecurity readiness. Cybersecurity readiness is critical for healthcare sector to sustain its operations, maintain its information technology (IT) system(s), protect against current and future cyber threats, and respond to and recover from a cyber-attack. Cybersecurity is not limited to the cyberspace, but incorporates the people, technology, processes and policies that contribute to an organization's overall cybersecurity readiness. This study developed a model that helps the hospitals to assess its cybersecurity readiness and provide recommendations on what should be done in order to improve its readiness in fighting cyberattacks.

1.3 The Statement of the Problem

According to Martin, Martin, Hankin, Darzi, and Kinross (2017) 81% of 223 organizations that were surveyed are at risk of being attacked and only half of these organizations think that they are able of fending off themselves against attacks. These prevalence of attacks is attributed to weakness in healthcare security posture. Over 10 million records were breached in US in 2015 alone and there has been a 300% increase in breaches over the past 3 years .These numbers portrays how the healthcare sector is vulnerable to cyber attacks. An example of a malware that wrecked havoc in 2017 included the WannaCry ransomware which affected more than 200 000 systems in more than 150 countries. Over 50 hospitals were directly affected in UK. These attacks affected care delivery, compromised patient's safety, and eroded the trust.

As the threat landscape on healthcare continues to escalate, many hospitals still lag behind in terms of protecting its critical infrastructure and electronic protected health information (ePHI) as evident in the use of outdated clinical technology, use of insecure internet enabled medical devices, poor security management process and excessive use of legacy technology (Wim, 2015). Vesely (2017) attributes the phenomenon to lack of funding to healthcare, poor infrastructure to track threats; difficulty in replacing legacy and vulnerable computer systems and unskilled technical staff to fight cyber-attacks. All these attributed challenges makes the healthcare sector vulnerable to attacks

In an effort to providing quality and efficient healthcare services to citizens, healthcare disregard necessary investment in securing its assets (people, process and technology) and thus putting patients information at stake. While it is clear that most

hospitals are vulnerable to attacks there is a need to develop a model that will help hospitals perform self-assessment in determining its readiness to fight the cyber-attack menace. The main focus for assessment is to help healthcare in maintaining its systems, sustain its operations, protect against current and future cyber threats, and respond and recover from it.

1.4 Purpose of the Study

The main purpose of this research was to design a web based application that will enable hospitals check their cyber security readiness index status based on the four pillars of cybersecurity; people, process, technology and policy. Cybersecurity readiness is critical for healthcare sector to sustain its operations, maintain its information technology (IT) system(s), protect against current and future cyber threats, and respond to and recover from a cyber-attack.

1.5 Objectives of the Research

The main objective of this study was to develop a model that would help in determining the cybersecurity readiness index (CRI) towards the adoption of eHealth for Hospitals. The main objective was directed by the following specific objectives;

- (i) To assess the cyber security readiness elements for adoption of eHealth
- (ii) To design a model to measure the cybersecurity readiness for eHealth
- (iii) To implement a prototype for computing cyber security readiness index as a web-based application
- (iv) To evaluate and validate the model

1.6 Research Questions

The researcher sought to find answers to the following questions;

- (i) How will the elements affecting cybersecurity readiness index in adoption of eHealth be assessed?
- (ii) How will the model for computing cybersecurity readiness index in adoption of eHealth be developed?
- (iii) How will the prototype for computing cyber security readiness index be implemented?
- (iv) How will the prototype for computing cyber security readiness index be verified and validated?

1.7 Significance of the Research

The study is be significant to the following stakeholders;

- (i) The research informs the hospital management on the level of readiness of the institution to fight cybercrime and also inform them on what should be put in place in order to avert cyber-attacks.
- (ii) The study also sought to raise awareness among the hospitals management on the importance of investing on information communication technology in securing patients information.
- (iii) This study sought to add existing literature on healthcare and information security management that will be of importance to academicians for further research and for building knowledge in the discipline.

1.8 Expected Outcome for the Study

The researcher intends to develop a model that will provide the following deliverables;

- (i) A model that would help in determining the cybersecurity readiness index (CRI)
- (ii) From computed CRI, the model will output downloadable recommendations that will help the management of hospitals implement necessary controls to safeguard the industry against cyber risks.

1.9 Justification for the Study

In an effort to ensuring confidentiality, integrity and availability of electronic protected health information (ePHI), measures must be put in place to protect sensitive patient information from cyberattacks. Healthcare sector has been the prime target for the past few years as attested by the escalated number of attacks experienced by hospitals lately. In 2015 alone, over 112 million records were breached and it's projected that the number will increase in the coming years (Drevin, Kruger, Bell & Steyn, 2017).The healthcare sector is becoming the centre of attack due to massive and sensitive data they possess. This cyber focus on healthcare has also been fuelled by proliferation of IoT devices in healthcare.

Apart from financial loss, hospitals reputation is damaged since patients trust on the institution goes down (Spence, Paul III, & Coustasse, 2017). To regain the confidence of the public in hospitals, management need to take the issue of cybersecurity with

seriousness it deserves. The study helps in identifying elements that should be safeguarded in order to protect patient's sensitive data.

Hospitals are among most sensitive sectors in the economy that should be protected by all means possible since it deals with people's lives. Attack on hospitals means that the lives of patients is at stake. As networked medical devices becomes more embedded in Hospitals, cybersecurity should also be prioritized in order to protect these medical devices from attack. While it is clear that most hospitals are vulnerable to attacks, there is a need to develop a model that will help hospitals perform self-assessment in determining its readiness to fight the cyber-attack.

1.10 Scope of the Study

This study designed a model to determine the level of readiness to cyber threats within Hospitals in Kenya by computing the cybersecurity readiness index. The study does not intent to overlap the existing studies but to improve.

1.11 Limitations of the Study

Due to sensitivity of the study, hospitals may be reluctant to give out all information as it is classified as confidential. However, the researcher assured the respondents of the secrecy of non-disclosure of information. Time and availability of resources are other factors that might limit the study

1.12 Scalability

The web model was implemented for hospitals in Kenya as a pilot environment. However, with the availability of resources the study will be scaled to cover other sectors and even extent to other countries.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature about cybersecurity readiness among hospitals. Specifically, the chapter gives us an overview of what needs to be protected and goes ahead to explore literature about the elements that affect cybersecurity readiness in hospitals namely; people, process and technology. Finally the chapter explores the research gap and the conceptual framework.

2.2 What needs to be Protected?

According to Ahlstrom & Zoline, (2018) healthcare has a large attack surface and at times it is complicated to know what needs to be protected. Figure 1 below summarises what needs to be protected in a healthcare.

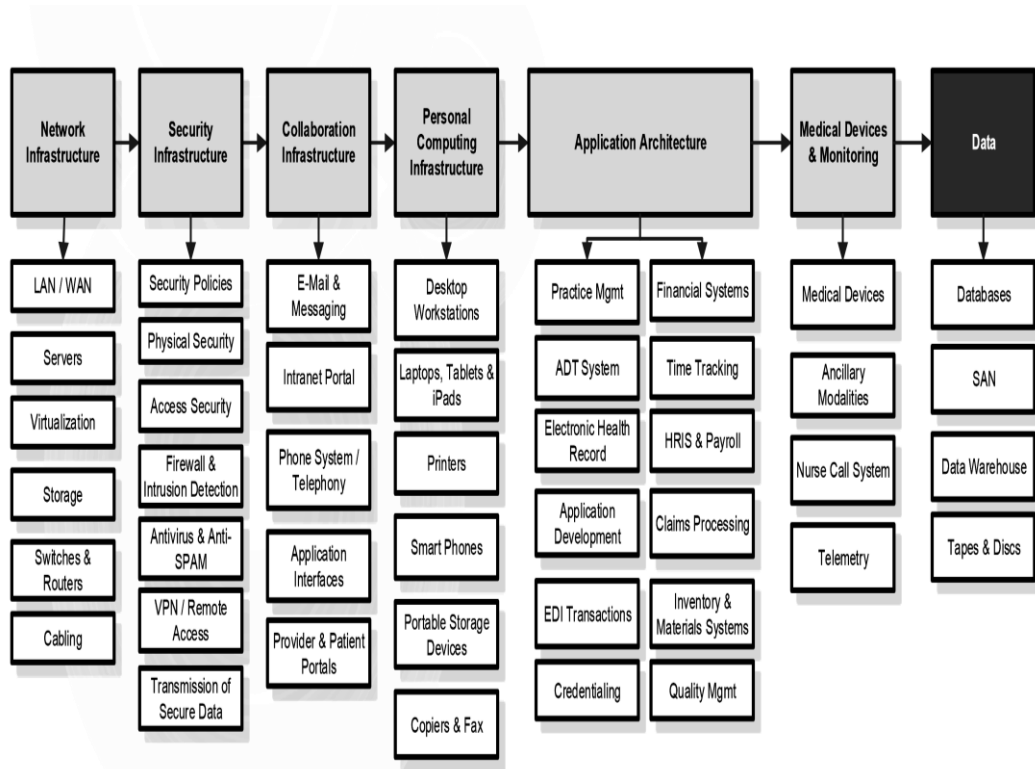


Figure 1: Healthcare attack surface
Source: Ahlstrom & Zoline, (2018)

The Figure 1 portrays a clear picture of what is at stake when healthcare cybersecurity maturity is low.

Cotenescu (2015) states that for an organization to increase its security posture, people, process and technology need to blend together.

2.3 People

People refers to employees, contractors, partners, suppliers and any party that has access to organizations data. People are considered the greatest assets to any organization because of the value they bring in. However, their access to sensitive information and assets make them the greatest inherent vector (Culp, 2016). According to Bulgurcu, Cavusoglu, and Benbasat (2010) people are considered the weakest links in security chain. ISO 27001's control 8 on human resource security considers people most vital since the security of information in any organization is the responsibility of the employees and third parties who have access to organization's information such as partners, suppliers and contractors. The increased number of parties that have access to information in an organization such as the healthcare industry increases the cyberattack surface and thus the exposure to cyber threats.

Organizations often believe that information security is solely an information technology (IT) problem and that technological solutions can address the stalemate (Janes, 2013). Unfortunately technology is not the ultimate solution to it. According to the report by Ponemon on information security, 59 percent say their organizations controls are not keen on monitoring contractors, employees and partners or other insiders who have access to confidential documents of the organization (Ponemon Institute, 2012). Users who have access to information are the root cause of many data breaches. Employees opening malicious mails, data loss on thumb drives, unsafe web browsing, re-use of passwords, careless handling of sensitive data such as leaving them exposed on their tables all demonstrate that human element is a major factor in data breaches and must be put in check before technology can make a difference. An organization can have the most secure systems in the world but still it can be breached by hackers. Hackers will always seek out the path of least resistance which is the human element. Stopping cyberattacks requires that organizations build a better defences around people.

According to Durbin (2016) security breaches as a result of human factors are categorised into three; malicious, negligent and accidental. Malicious act is when an employee, contractor or a partner intentionally does something with the motive of harming the organization such as turning over sensitive information to a competitor.

Malicious behaviours majorly occurs among disgruntled employees. Negligent behaviours occurs when people find ways to avoid policies they feel it is unfavourable. While most have a general awareness of security risks and recognize the importance of compliance, their workarounds can be risky. Accidental behaviours occurs when employees accidentally perform acts that may harm an organization unknowingly such as emailing sensitive data to a wrong recipient. According to the report by Verizon data breaches, accidental account for almost 30 percent of information security incidents.

According to Kenya cyber security report (2015) over 80% of system-related breaches were perpetrated by insiders who include disgruntled employees. The report goes on to portray that in 2016, over 50% of direct costs of cybercrime was attributed to insider threats (Serianu, 2016). In as much as people are considered the main culprits of security breaches, they can also be the targets in the event, KPMG Cyber Crime Survey of 2015 for instance indicated that 64 per cent of security breaches in many organizations targeted directors and senior management.

For a holistic approach to management of Information Security, security must focuses on technology, processes, policies and people. Many organizations put a lot of emphasis on securing technologies and process neglecting the most important element of security, human factor. Information security therefore a human challenge and that means that it is the people who develop the culture of the organization and therefore custodians of security (Ashenden, 2008).

2.3.1 Awareness and Training

The healthcare sector is arguably one of the most information-intensive industry. Personal health information is critical pathway that affects our daily lives and health. The confidentiality and integrity of these health records is paramount, not only for well-being of individuals but also for continued innovation within the sector. Healthcare industry being part of massive data revolution, at a time when cyberattacks is wreaking havoc means the sector is a prime target. FBI have warned that healthcare sector is not resilient as other industries such as financial and retail sectors and thus most likely to be attacked.

The healthcare industry has experienced a lot of changes with the electronic records coming in place to replace the traditional paper-based medical records. This shift has

improved the provision of healthcare services, minimised insurance fraud and also reduced billing errors. However, the shift to digital mode calls for additional awareness and responsibility by healthcare professionals to protect the sensitive information against possible data breach. Many healthcare employees might not be fully aware of the cybersecurity risks facing the industry. Employees should regularly be informed and reminded of the vulnerabilities and risks they face ranging from patients safety, reputation damage to huge financial losses (Williams, 2016). With all the variables coming in play, healthcare industry needs to take a pro-active approach in building a program of cybersecurity awareness. Cybersecurity awareness uses knowledge and education to tackle cybersecurity threats, in all its forms. Security awareness and training covers the whole scope of security and establishes a knowledge base across extended workforce around cyber risks that can call upon help to mitigate. Employees are the last safeguards against medical data breach.

The rapid digitalization of healthcare makes building an effective cybersecurity awareness programme a challenge due to a lot of devices connected sending and receiving endless amount of data records. Recent report indicates that 75 per cent of healthcare industry was hit by malware attack in 2016. While many large attacks involve hackers, Health IT Security reports that most of costly breaches in 2015 originated from misconduct, including mishandled data and stolen devices. Due to massive adoption of BYOD and wearables in the healthcare sector, training and awareness among the employees is paramount less the industry continue to suffer medical breaches.

Awareness and training among the healthcare employees should be conducted on a regular basis, this is due to dynamic nature of cyber threats. The awareness and training should be reviewed regularly to focus on problem areas and keep up with new threats (Janes, 2012). Training and awareness should have metrics to measure the impact of the program to the users (Olavsrud, 2012)

2.3.2 Importance of Security Awareness and Training

The main focus of healthcare professionals should be providing quality healthcare services to their patients, they cannot disregard the importance of securing patients information. The motto of health IT is to provide faster, more efficient and more cost-effective care to patients through the use of improved hardware and software technologies that already proved efficient in transforming other industries according

to InfoSec institute. However, cyber risks should be considered, and enough security provided. Security awareness among the healthcare professionals is essential part of security measure to be undertaken in order to secure the industry critical system. Institute and Resources outlines some of the importance of training and awareness as;

Training and awareness creates a culture of proactive cybersecurity among the healthcare staff. The best defence against cyberattack is knowledge, and it comes with training and awareness. Joe Ferrara, CEO of wombat technologies believes that organizations can reduce cyberattack between 45 percent and 70 percent by implementing training programs that include assessment, education, reinforcement and measurement. Training and awareness enables employees and executive to recognise signs of threats such as phishing, social engineering as well as to avoid mistakes as downloading files without proper checking. This equips them with proactive security mind.

Training enables employees to know what protected health information (PHI) is and reasons it should be protected. PHI contains sensitive patient's information such as bank account number, medical record numbers, health insurance numbers and other sensitive information as outlined by health insurance portability and accountability act (HIPAA). Such information may be used for medical identity theft (Andrews, 2016). Making staff aware of the importance of PHI information enables employees be careful when handling such data to avoid cyber human error.

Training and awareness makes staff know which security and privacy rules apply to healthcare and what impact they have. Training is the only avenue that staff are made to know the rules governing the privacy and security of the healthcare industry because they get to interact and ask questions to the experts. Other benefits of training and awareness include; makes staff understand that security is part of the whole organization and impacts everyone and also enables staff build respect towards the privacy of individuals.

Healthcare industry has a lot of things to look after, such as providing quality healthcare service to patients, retaining financial viability as well as leveraging information technology (IT) to upgrade the operational standards. Still, healthcare industry has to give equal priority towards maintaining high-quality security settings to prevent any possible data breach. Raising cyber security awareness among health

care professionals also involves making them aware of the consequences of errors in individual actions (such as clicking malicious links that can compromise the whole network and lead to data breach).

2.3.3 Human Resources Security (ISO)

As stated in many sources, people are regarded as the weakest links in security chain. According to Kigen et al. (2015) 80 % of the breaches experienced in Kenya was attributed to insider threats. ISO 27001 control 8 on human resource security plays a massive role in ensuring that human resource is kept in check prior employment, during employment and during termination or change of employment. Many organizations put a lot of emphasis on securing technologies and process neglecting the most important element of security, human factor. Information security therefore a human challenge and that means that it is the people who develop the culture of the organization and therefore custodians of security (Ashenden, 2008).

ISO 27001's control 8 establishes standard requirements an organization should comply with prior to, during, and after termination or change of employment for employees, contractors and third parties.

a) Prior to Employment

The core objective of this control is to ensure that contractors, employees and third party users understand their roles and responsibilities in accordance to stipulated information security policy (Calder &Watkins, 2008). The control requires one to protect the information assets of the organization from disclosure, modification, use and unauthorized access. In this case, the control requires that candidates considered for employment, third party user status or contractor status must undergo screening with respect to appropriate ethics, laws, perceived risks, and classification of information to be accessed. The control also stipulates that employees, contractors and third party users must agree to terms and conditions of the employment by signing statement of rights and responsibilities including rights and responsibility in regard to information security.

b) During Employment

Control A.8.2 of ISO applies to employees, third party users and contractors who work together in ensuring that the goals of the organization are achieved during the period they are working with the organization. This basically requires that the

employees, contractors and third party users understand their security responsibilities with regard to protection of information assets in the organization. The core objective of this control is to ensure that contractors, employees and third party users are fully aware of information security threats and are ready to support the management in applying security controls in accordance to organization's laid down policies and procedures.

The control also requires that employees of the organization must undergo regular security awareness and training in order to create a culture of proactive information security within the organization. Lastly, the control stipulates that the organization must establish formal disciplinary process for the employees who are involved in a security breach.

c) Termination or Change of Employment

The objective of this ISO control is for the purpose of ensuring that employees, contractors and other third party users exit the organization or change employment in an organized manner. In this case, responsibilities for doing termination or change of employment for the affected employees and contractors must be defined and assigned clearly, this enables other employees and contractors to be informed of persons change in status. Upon termination or change of employment the control requires that the affected person returns all the organization assets in their possession, this includes the software, hardware or data of any kind. In the case where the employees or the contractor are allowed to use personal device such as laptops and phones (BYOD) organization's data and software must be securely erased. The process of assets return must be formalized. Lastly, the affected persons access rights must be revoked and given new access rights the case of change of responsibilities within the organization

2.4 Process

IT governance defines a process as a structured set of activities designed to accomplish a specific objective. It can take one or more defined inputs and turn them into a defined output. Even with the best people and technology in place one cannot be safe from cyber-attacks unless there are well defined processes in place which identify procedures, roles, activities and documentation should exist to mitigate the risks associated with cybercrime. According to Bayuk (1997) effective security management process is comprised of six sub processes: awareness, access, monitoring, compliance, policy and strategy.

2.4.1 Awareness Process

Process awareness describes a degree to which the awareness participants are conversant with the process requirements, procedures, workflow, rules and other details. Good security awareness of the staff is paramount condition for the success of any organization since it ensures that employees do what is expected of them. Employees act effectively if they feel their duty and know their contribution in terms of the whole process goals. The higher the process awareness, the more overwhelmingly the employees are engaged into a process, and so the much better results they deliver. The need to incorporate training and awareness is not only to provide awareness but provide instructions for users to follow based on specific circumstance (Jane, 2013).

The core function of security awareness is to promote security, inform the employees on the security developments, and establish accountability. Awareness focuses mainly in getting maximum attention of workforce on security issues. Workforce needs to continuously be pushed to be aware of security policies in different formats. Security awareness program includes communication, tools and communication developments.

Security personnel is charged with the responsibility of creating a security awareness program which is implemented at the department level by the department liaisons. The awareness program should be comprehensive, flexible, clearly communicated and easily understood by the department liaison.

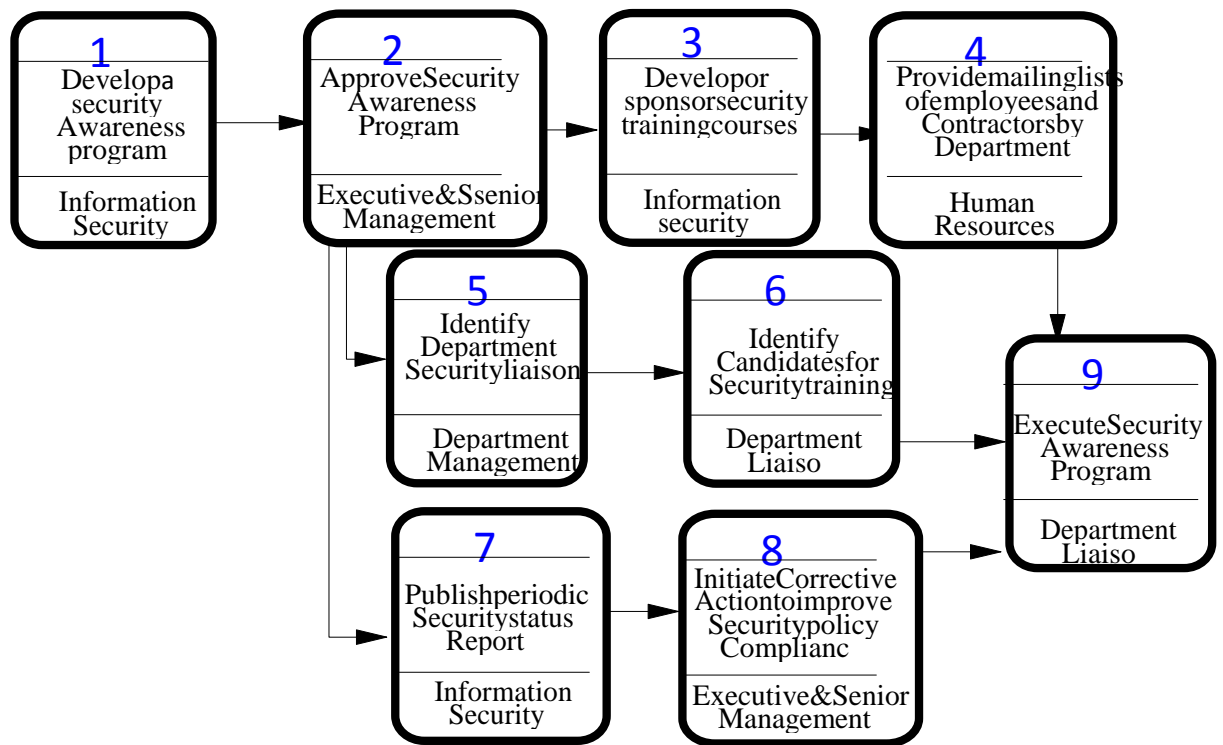


Figure 2: Awareness process
Source: Bayuk (2012)

2.4.2 Access Process

According to Wiech (2015) data security is of paramount importance in the healthcare industry, where spot on access rights for information is critical. Electronic medical record (EMR) which allows for the collection, management, extraction and sharing of information contain sensitive data about patients and should be protected from security breach at any cost. Breach to EMR not only has financial and reputation effect but could be devastating for the patients due to the nature of information disclosed.

A security access process ensures that decisions made on who should access what type of information and who should not. The process also ensures that information concerning access is communicated securely to those intended for. Access process should be able to address the identification of those in need of access, authorization procedure and authentication (Bayuk, 2012).

a) HIPAA Information Access Management

According to Health Insurance Portability and Accountability Act (HIPAA) access to electronic protected health information (ePHI) must be guarded to ensure confidentiality, integrity and availability. Security rule requires appropriate

administrative, physical and technical safeguards to guarantee against any illegal access to information. Administrative safeguard on information access management standard outlines the implementation needs of a covered unit concerning to protection of health information while allowing access. Administrative safeguard has three specifications; isolating healthcare clearinghouse functions, access authorization and access establishment and modification.

(i) Isolating healthcare clearinghouse functions

The HIPAA information access management under security rule stipulates that if the clearinghouse of a healthcare is part of the larger organization then procedures and policies must be implemented by the clearinghouse in order to protect electronic protected information of the clearinghouse from unauthorised access by the larger organization

(ii) Access Authorization

The access authorization policy is meant to protect electronic protected information (ePHI) which is currently available and that which may be created. HIPAA requires that authorization access must be documented and implement procedures and policies for granting access to ePHI; for example through access to transactions, workstation, program, process or other mechanisms.

Guidelines to be followed when putting into implementation the policies and procedures for access granting to ePHI include, and not limited to the following; most security breaches of confidentiality is as a result of poor personnel security, which is majorly because of poorly information access authorization. Therefore, the unit responsible for managing authorization must ensure that access is limited to minimize the risk, HIPAA accreditation specify that only those in need of the access and use of PHI should have access to such information, those with authorized access to information should have no more access privileges than needed for the performance of their duties, emergency override may be required for some ePHI users such as nurses and physicians in case they want to respond to an emergency finally HIPAA requires that all personnel with access should be screened.

HIPAA requires that healthcare develop and implement procedures and policies for granting and maintaining privileges for personnel to access electronic confidential information. The information technology administrator or any person responsible for granting authorization should document and maintain such access authorization

records. The covered entity should document authorization for access and level, defined time and document roles. When non-workforce personnel use the computer for maintenance or hardware installation, they need authorization, and should be required to sign and date the required documents

(iii) Access Establishment and Modification.

HIPAA security rule policy on access establishment and modification requires that policies and procedures be implemented. Once access has been granted, the covered entity should consider implementing procedures and policies to establish that access and to modify that access in the future as required. The core objective of access establishment and modification is to constitute policies in accordance with the entity's documents, access authorization, establish, modify, and review a user's privilege to access transaction, program, process or workstation. Access control and monitoring are vital features in granting access to electronic protected health information and at any point in time. It is important to capture information on who logged in to the system and in what level of privileges and also the changes made to the data by respective persons.

According to ClearWater Compliance, access establishment majorly concerns the security rules and policies which defines an entity's initial right of access to terminal, process, transaction and program. Access modification on the other hand concerns the rules and policies that defines the kinds of, reasons for, modification to an entity right of access to terminal, process, transaction and program.

Access establishment and modification policy is not a mandated policy but rather a compliance. The specifications for access establishment and modification for access authorization is addressable. According to Ferran (2014) addressable should not be misconstrued to mean optional but the decision not to address a specification should not be made casually. The extent to which these specifications will be put in place will have to be based upon other issues such as; the organization's size, cost, technical infrastructure and complexity, degree of automation and risk management strategy. A covered entity which is fully automated and its infrastructure spanning across multiple locations with a lot of employees may adopt a formal policy for access authorization

while smaller may decide to have a desktop standard procedure that will meet the specifications.

The procedure should be able to describe how access is actually implemented through the use of different systems and procedure, comprising of passwords and card keys. An access authentication policy should create trust through an operational password policy, and by putting up guidelines for remote location and use of authentication devices. An accountability policy describes the duties of users, management, and operational staff. It should stipulate the capability of the audit, and specify incident handling procedures as required.

The organization should monitor access to ensure individuals have access to the ePHI they need and no more. If an individual has too little access, access should be authorized and expanded. If they have too much access, access needs to be restricted. The Security rule does not dictate a particular access control mechanism, however, user-based, role-based, and context-based access control procedures are the most prevalent and widely used. Consistent access management is a critical component in having effective security. Ensuring that workforce members and other users only have privileges required to perform their job functions mitigates a great deal of risk, as the greatest threat to security has always been the insider.

2.4.3 Compliance Process

Sadiq, Governatori, and Namiri (2007) defines compliance as a process of ensuring that business processes, operations and practice are in accordance with the required norms. Compliance stems from regulatory bodies (HIPAA, HITRUST) or from recognized standards (ISO, NIST). According to Bayuk (1997) the degree at which compliance process has been formalised is the extent at which security management determination are effective in forming a uniform level of security controls.

To create an effective healthcare compliance program, hospitals must adhere to 4 principles (Budryk, 2015). The relationship between the audit, compliance and legal department must be defined clearly. Healthcare management must state each department boundaries and responsibility so as to avoid conflicts in compliance process. Secondly, each compliance related sector should independently report to the hospital management on its risk management and compliance. Thirdly, hospitals

should identify and audit probable risk areas, this should be followed by immediate corrective plans in order to avert risks before it happens. Auditing and monitoring helps in identifying potential vulnerabilities and compliance concerns. Lastly, compliance should be encouraged throughout the hospital.

2.4.4 Capability Maturity Model (CMM)

Capability maturity model (CMM) was developed by software engineering institute (SEI). The main purpose of CMM development was to provide organizations an approach of developing and refining its processes based on a process model (McKay, 2016). Process model is a set of practices that defines the characteristics effective processes; these practices include the ones that have been proven to be effective by experience.

CMM provides a scale of five process maturity levels which an organization can assess itself against it. Each process maturity level ranks an organization in respect to its standardization of process the assessed subject area. The subject areas to be assessed can vary as systems engineering, information technology, software engineering, project management, system acquisition, and personnel management (Mckay, 2016). CMM model recognises five process levels for an organization. Within each of the five process maturity level are key process areas (KPA) that characterise that level, and for every KPA there are five definitions identified from the first one; goals, commitment, ability, measurement, verification consecutively. The maturity levels are measured by the accomplishment of the generic and specific goals that apply to every predetermined set of process areas (György, 2012). The five levels of CMM include; initial, repeatable, defined, managed and optimizing.

According to Abigail Heller a research specialist, there exist several reasons why organizations use process management maturity model and they include; it increases visibility of the processes to proven since the process have been proven effective from best practice organizations, creates a structure that defines what tasks are needed to be done, when and who to do it, facilitates a collective dialogue concerning process management and finally process management maturity model enables process use and capture in a consistent manner.

a) **Maturity level 1: Initial level**

It is characteristic of processes at this level to be ad hoc, undocumented and at a state of dynamic change tending to be driven in an ad hoc uncontrolled and reactive manner by events or users. This provides a chaotic and unstable environment for the processes. The success of processes at this level entirely depend on the employees' expertise, talent and heroics rather than the implementation of proven processes. Organizations at this level have a tendency of abandoning the process in time of crisis. Though process work at this level they frequently exceed the budget.

b) **Maturity level 2: Repeatable level**

In this level the basic project management processes are established and necessary process discipline is in place to repeat early success projects with the same applications. Some processes are repeated with the possibility of consistent results. Process discipline is in place but it is unlikely to be rigorous. However, existing best practices are retained to be applied during times of stress. At this level, practices are in place and projects are implemented according to documented plans. Processes, work product, requirements, products and services are able to be managed. Work products and services at the repeatable level the requirements, objectives and standards

c) **Maturity level 3: Defined level**

At level 3 processes are standardised, documented and integrated into all available process for the organization. At this level we can see sets of determined and documented processes which are subject to some level of improvement over period of time. Processes at level 3 are well understood and are described in standards, tools, procedure and methods. The main difference between level 2 and level 3 is that, in level 3, processes are described in a more detailed and more rigorous than in level 2. Further, processes are managed with the knowledge of interrelationships of the processes and products, measures, and services. Also processes are predictable but there are no measurements to enforce.

d) **Maturity level 4: Managed level**

Detailed measures of processes and their outputs are collected, quantitatively understood and controlled. Using process metrics management can now effectively control the process as well as identifying ways to adjust and adopt to the processes to particular projects without loss of quality. A clear distinction between maturity level 3

and maturity level 4 is that the process performance are more predictable in maturity level 4. Sub- processes at this level contribute to the general performance and are controlled using quantitative and statistical techniques. Finally, measurements are centred on what the customer, end user, organization needs in an effort to support decision making in the future.

e) **Maturity level 5: Optimizing level**

At this top level of maturity model, process are undergo continuous improvement through both incremental and innovative technological improvements to increase process performance. At this level the organization is able to identify the strengths and weaknesses of the process proactively, with the aim of preventing defects. Data collected from the process effectiveness is then used to perform cost benefit analysis of the technology and may suggest change to the process (Paulk, Curtis, Chrissis, & Weber, 1993).

2.5 Technology

Technology cannot be deployed without people, processes and policies in place. However, technology plays a critical role in cyber security as stipulated by the It Governance. By identifying the cyber threats that the organization faces provides a way of knowing the controls to be put in place and the technology needed. In September 2012, the government of UK in conjunction with cabinet office and communication electronics security group (CESG) released 10 steps to cybersecurity guidance. In 2015 the guidance was updated and simplified to cope with evolving cyber threats. If the guidance is implemented as a set then cyber threats will reduce significantly by helping to prevent the majority of the attacks. As expected the guidance involve people, process and technology. Of the 10 steps, 6 are technology related elements. They include; network security, managing user privileges, malware protection, secure configuration, removable media controls and home and mobile working.

2.5.1 Network Security

Network security can be defined as the process of taking software and preventive actions to protect the networking infrastructure from misuse, malfunction, unauthorized access, and modification in an effort to create a secure environment for the functioning of computers, users and programs. Network in our case refers to both internal and external network. With the implementation of physical, administrative and technological controls network security management tries to create a safe

environment established upon the layers of protective component that work in conjunction to enhance general security.

According to Golchha, Deshmukh, & Lunia (2015) major attacks to network include: active attack, passive attack, insider attack, close: in attack phishing attack, hijack attack, password attack, denial of service attack etc. However, a secure system should be able to minimise damage and recovery methods when an attack occurs. Some of common solutions to these attacks are; network access control, firewall, network monitoring, intrusion detection system and intrusion prevention system.

a) Firewall

A firewall is security device that provides a mechanism for filtering incoming packets and outgoing packets. Based on the policy rules firewall can decide whether to deny, allow or take action on the packet. Firewall is considered as core elements in network security (Golchha et al., 2015). The effectiveness of a firewall depends on the design of firewall security policy, a well-designed firewall security policy is capable of protecting the network while a badly designed firewall design policy may led to firewall accepting malicious packets and rejecting acceptable packet (Golchha et al.,2015). Firewall can be implemented as software, hardware or a combination of both.

(i) Simple Packet Filter

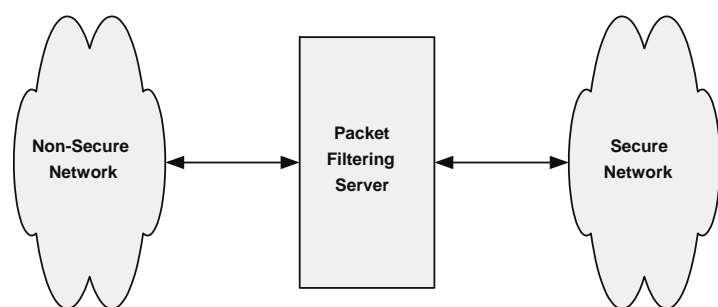


Figure 3: Simple Packet Filter
Source: Kumar and Singh (2014)

This type of firewall applies a set of rules called access control list (ACL) to every incoming and outgoing packet to determine either the packet should be forwarded or discarded. Filtering rules are based on information contained in the packet. This

information include; source and destination IP address, destination transport level address, IP protocol field, and interface. If packet matches one of the rules, then role is invoked else if there is no match then default rule is invoked. Default rule can either deny (discard all packets except the allowed rule) or permit (forward all packets excluding the denied one). Packet filter is stateless meaning it does not maintain the results of the previous packets. Some advantages of packet filter is that it is very fast since it only checks the TCP/IP header, simple and transparent to users.

(ii) Application Level Gateway

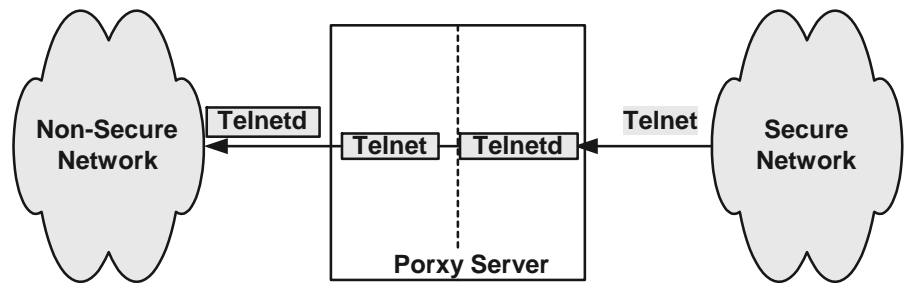


Figure 4: Application Level Gateway
Source: Kumar and Singh (2014)

Application level gateway is also known as the application proxy. In proxy level gateway, the communication between the user and the remote host is through the application program that run on a firewall that sits between the internal and external network. Proxy establishes connection to the remote host behind the firewall and acts on behalf of the user, this helps to protect the client computer on the network behind the firewall. Proxy server establishes two connections, one between the client and the proxy server and the other between the proxy server and the remote host. The two connections slows down the communication due additional processing overhead. Application level gateway tend to be more secure than the packet filter because the proxy is aware of the application protocol and can use it to allow or restrict packets

(iii) Circuit Level Gateway

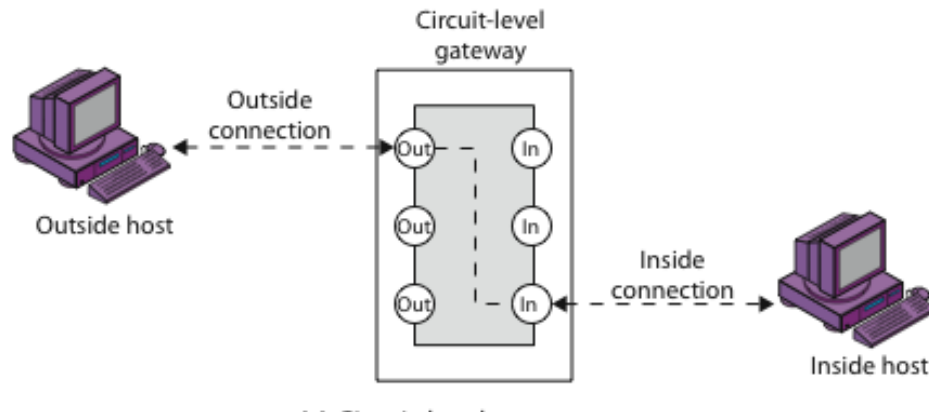


Figure 5: Circuit Level Gateway
Source: Kokko (2017)

A circuit level gateway does not allow end-end TCP connection but works by establishing two TCP connection, one connection between itself and inside host and the other connection between itself and the outside host. The purpose of the firewall is to intercept TCP connection to the host behind it and complete the handshake on behalf of this host. The circuit level gateway is always deployed at the session layer of the OSI model.

b) Network Access Control (NAC)

The main purpose of NAC is to protect network from unauthorized access this serves to identify and secure access to network critical infrastructure. ISO 27001 (2013) breaks down network access control into seven sub- controls; policy on the use of network services that stipulates that a user can only access specific network services they have been authorized, user authentication for external connection that requires remote users to be authenticated using appropriate methods, remote diagnosis and configuration and configuration ports, equipment identification in networks that require the automatic identification as a means of authenticating connections from specific equipment and locations, remote diagnostic and configuration port protection for controlling physical and logical access to diagnostic and configuration ports, network segregation, groups of information services, and users, groups of information services, and users, network connection control to restrict connections in shared networks, and network routing control to ensure that information flows and computer connections do not violate the access control policy of the business applications.

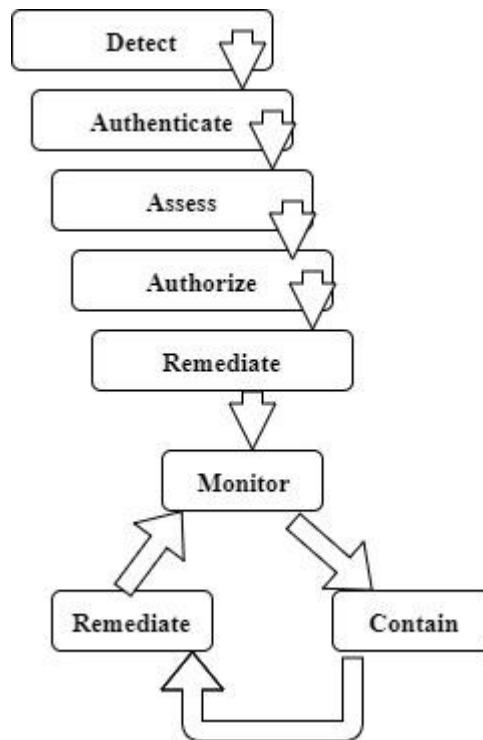


Figure 6: Access Control Process
 Source: Enterasys secure networks (2016)

c) Authentication, Authorization and Accounting (AAA)

The main purpose of AAA is to enable mobility and dynamicity in security (Convery, 2009). According to Convey, the absence of AAA means networks must be configured to control access; IP addresses must be fixed, systems are permanent meaning they cannot move, and connectivity must be appropriately defined. The proliferation of digital devices such as mobile devices, increased network consumers, and diverse methods of accessing network as necessitated the adoption of AAA process.

According to Gardner (2009), authentication involves the process of validating the end user identity before access to network is granted. Authentication may involve use of a combination of username and password, secret key or biometric data (fingerprint for example). The commonly used form of authentication is the use of a username and password. The user keys in the password and username which is compared to the credentials stored in the database. If the credentials match then the user is granted access to the network.

Authorization defines what services and rights are allowed to the user once authenticated to access the network. Gardner (2009) defines authorization as a process adding or denying a user access to network and its resources. An individual may be granted access to a network but with limits. Authorization to a network is based on time of the day, geographical location restriction, frequency of logins by individual. Authorization can range from simple as making sure that users has signed in to sophisticated checks concerning user role, group, or computer logged in from.

Accounting is tasked with keeping records and tracking user activities on a network. For a specified time period but not limited to, time spent accessing the network, network resources accessed, billing data, login data, network cost allocation and amount of data transferred or accessed.

d) Intrusion prevention system (IPS) and intrusion detection system (IDS)

With increased network attacks, layered security is essential for prevention of attacks. Layered security is possible through the implementation of intrusion prevention system (IPS) and intrusion detection system (IDS). IDS is a system defence which monitors traffic in the network by identifying intrusions, attacks and malicious activities a then generate an alert to the administrator in case there is any unusual activity that might compromise the security of the network (Patil, Rane, & Meshram, 2012). IDS can both be implemented as a software or as a hardware. IPS on the other hand monitors the traffic on the network just as the IDS but what makes it unique is the ability to prevent attacks apart from generating alerts (Ashoor & Gore, 2012). The main difference between IDS and IPS is that IDS only generate alerts when the attack has been but, IPS on the other hand detect and rectify errors (Charaborty, 2013).

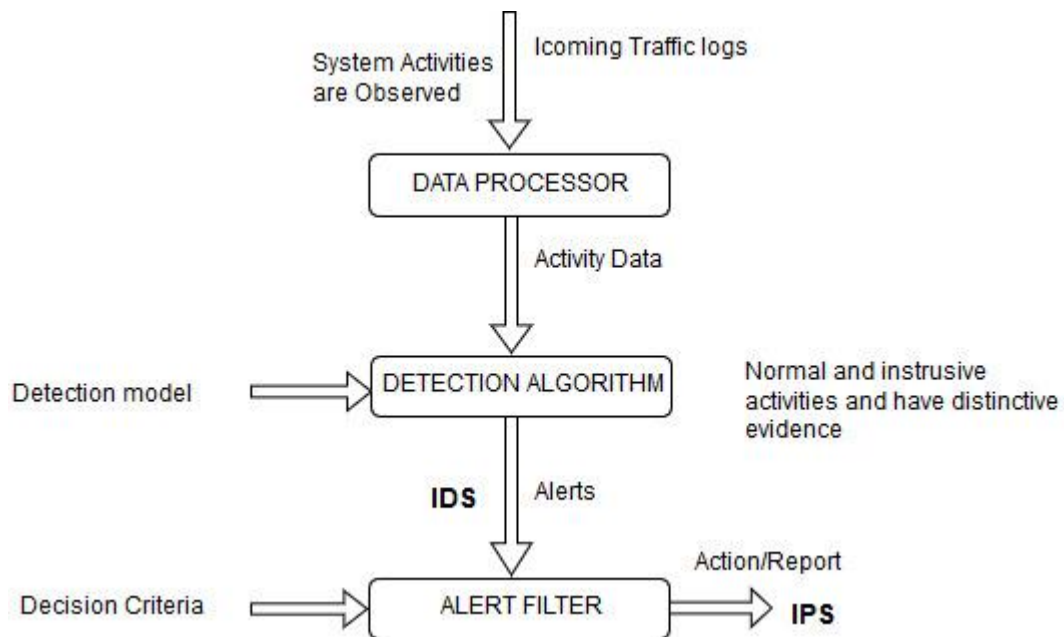


Figure 7: Role of IPS and IDS in network security
Source: Chakraborty (2013)

2.5.2 Managing User Privileges

National Cyber Security Centre (2015) defines user privilege management as the process of granting system privileges or data access rights to users depending on their roles. Privilege management provides a way of balancing between user productivity and security. Granting unnecessary access to users results in deliberate or accidental misuse of privileges by compromising with user accounts, it also elevates the attacker capability since the user can compromise other redundant accounts and use them to facilitate an attack. User privileges can be managed through; establishment of effective account management process, this enables the review of accounts from creation, modification and deletion of accounts that are unused or accounts created for temporary workers; limiting the use and number of privileged accounts, this ensures that privileged accounts such as system and database are reviewed regularly than normal accounts, limiting user privileges, conducting personnel screening, having in place policies to guide access control and identification and finally all users should be monitored.

a) Privilege Escalation

Privilege escalation or privilege elevation is the act by which a user gains access to resources that are not entitled to access. Authorization mechanism is intended to protect the resources (Kane, 2015). Privilege escalation is categorized into two; vertical privilege escalation and horizontal privilege escalation. Vertical escalation is where a user uses the existing access either illicit or granted to gain access to resources that is beyond what the current user is allowed to access. Vertical escalation is normally described as the act of elevating from “normal user” to “administrator” privileges (Alfaro, 2016). Horizontal escalation on the other hand is where a normal user with ordinary privileges exploits system vulnerabilities to access resources or content reserved for user with the same privileges.

2.5.3 Removable Media Control

Many organizations rely on removable media to conduct business due to the mobility of workforce today. The use of removable media in workplace is at a rise and measures to safeguard organizations data should be put in place. According to Freeborn (2017) many security teams majorly focus on detecting exploits, prevention of malicious code, and hardening infrastructure but they forget to secure and monitor removable media which plays a significant role in data loss. Removable media is one of the known source of malware infection. Latest report shows malware is among the leading cause of data loss in many organizations. Cyber advisory service stipulates some of the measure to protect data loss through the use of removable media, some of the measures include; formation of corporate policies that guides on the use of removable media in the organization, limiting the use of removable media, scanning media for malware before importing or exporting data in organizations systems, encryption of data in the media to protect data loss in case the removable is lost, locking down access to media drives to only allow authorized removable media, and finally educate users and create awareness on the risks of inappropriate and careless handling of removable media.

2.5.4 Malware Protection

SANS institute (2014) defines malware as a software, computer program used to perform malicious actions. In fact, malware is a combination of two words malicious and software. In 2016 ransomware wreaked havoc to healthcare sector. Latest report released by Verizon Data breach Investigation shows that 75 percent of the attacks

that were experienced in healthcare sector in 2016 were all because of Ransomware. This calls for strict measures to be undertaken in order to protect our healthcare against malware attack. This measures includes formation of policy and establishment of anti-malware defences.

a) Malware defence approaches

Rajab, Ballard, Lutz, Mavrommatis, and Provos (2013) states some of the approaches to curb malware attack as;

Content-based detection: antivirus software is an example of content based detection technique. Antivirus software run on end user system and it employs signature based technique to guard against malware attack. Antivirus software suffers a lot of setbacks such as development of sophisticated evasion techniques that can circumvent detection by malware authors. Another setback experienced by antivirus is the ability to detect new malware variants.

Blacklist-based protection: blacklist based protection approach provides protection by blacklisting malicious sites that may infect users with malware. The approach integrates with the browser.

Whitelist-base schemes: contrary to blacklist, the whitelist approach allows only those benign software to be installed and installation of any other software is disallowed.

Reputation-based detection: several research have been done on how reputation technique protects against malware. Hao, Syed, Feamster, Gray, and Krasser (2009) proposed SNARE, reputation technique for protection against spam emails. Qian, Mao, Xie, and Yu (2010) proposed use of network based.

2.5.5 Secure Configuration

Secure configuration refers to measures that can be implemented when building or installing a computer or network device that serves to minimise cyber vulnerabilities. According to Open Web Application Security Project (OWASP) even a robust system becomes weaker when it's misconfigured. Secure configuration involves applying security patches and ensuring that all information technology systems are maintained. Some of measures to avoid misconfiguration include; having documented installation process, proper file and directory permission, having documented configuration management systems for networks, conducting regular network scans to check on vulnerabilities and avoiding unnecessary software installation.

2.6 Policy

Cyber Security Policy is a formal set of rules made to govern those who have access to company technology and information assets. The main purpose of a policy is to inform users: contractors, employees and other authorised users of their obligatory requirement to protecting information assets. Cybersecurity policy describes the information assets and technology that must be protected and identifies threats to those assets. The policy also states the user's privileges and responsibilities. Finally Cybersecurity dictates user's limitations and notifies users of the consequences when the policy is violated and provides the procedures to be followed when responding to an incident that threatens company computers system and network. In light with the increased number of cyberattacks, companies are needed to have policies with respect to data retention, privacy, data protection and data destruction (Schaeffer, Chan, Chan, & Ogulnick, 2009)

2.6.1 Security policy components

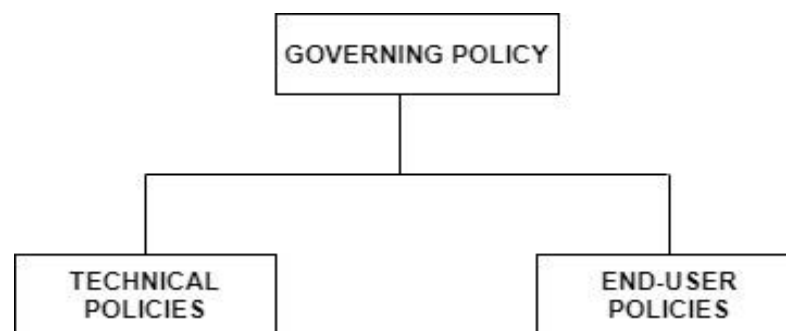


Figure 8: Network Security Concepts and Policies
Source: Pearson education (2017)

a) Governing Policy

This security policy is the top level security concepts that are paramount to the organization. The governing policy is meant for the technical team and the managers. It controls any security policy-related within the departments and business units. The governing policy tries to answer the question “what”. (Cisco press, 2016) outlines some of the components of a governing policy as; it should state how the policy should apply in the environment, consequences of non-compliance, which actions processes, actions and activities are allowed and which ones are not, the level of compliance should be outlined.

b) End-user Policies

This security policy document outlines all security topics related to the end users. The policy answers the “who”, “when”, “what” and “where” security questions. End user policy covers all important topics pertaining to information security that the end user should comply with, know about and implement. A times this policy may overlap with technical policies. The grouping of all end-user policies is to make it easy for the user to access all policies pertaining information security at one place.

c) Technical Policies

The policy is majorly meant for the technical staff. The purpose of the technical policy is to guide the staff in protecting the systems from security breaching. The policy is more detailed than the governing policy. Technical policy answers the questions “what”, “when”, “who” and “where”. Some of the typical policy categories of technical policy include; general policies (audit policy, acceptable use policy, password policy, risk assessment policy global web server policy), email policies, personal device and phone policies, remote access policies (dial-in access policy, VPN security policy, remote access policy), network policies (extranet policy, network access standards, wireless communication policy server security policy), application policies (application service provider policy, and database credentials policy source code retention policy, acceptable encryption policy)

2.6.2 Acceptable Use Policy

According to Navex Global (2016) acceptable use policy outlines the acceptable use of electronic devices and network resources within an organization. The rules outlined in the acceptable use policy is meant to protect company’s information assets against loss, theft, copying, unauthorized access, modification or destruction. With the increase in cyberattack, responsible use of internet is a mandate for every person. Acceptable use policy dictates the dos and don’ts while using internet resources. Acceptable use policy should be communicated to the employees. Employees should read the policy and sign it. Obtaining the consent of the employees is to protect them from taking liability in case of a misuse. Examples of acceptable use include; email acceptable use, internet acceptable use and secure extranet acceptable use.

2.6.3 Encryption Policy

Encryption policy ensures that information or data on transit or at rest are properly encrypted against unauthorized exposure, loss, or unauthorized changes. Data at rest refers to data that resides locally in the database or in a computer while data on transit refers to data that is moving through a network of wireless devices. Data on portable devices (. smart-phones, flash, SD cards, USB file storage) should also encrypted in case of loss. Protected health information (PHI) should always be encrypted since it contains sensitive patient's information. According to HIPAA rules, encryption is an "addressable" requirement, this does not mean that encryption is optional but rather if one chooses not to implement encryption then equivalent solution should be implemented in order to meet the regulatory requirement.

2.6.4 Information Security Policy

The main objective of information security policy is to provide confidentiality, integrity and availability of information. For the case of healthcare, information security policy serves to protect health information entrusted to the hospital by the third party who are the patients. Information security management system (ISMS) provides a systematic approach for securing sensitive information. According to Kosutic (2016) some of the components information security policy include; policy has to be adopted to the organization meaning one cannot copy the security policy of one organization and apply in another organization. Secondly, the policy needs to provide a framework on how the policy objectives are proposed how they are reviewed and approved. Thirdly, the policy show the commitment to improve the ISMS and fulfil the needs of other interested parties. Fourthly, the policy must be within the organization and any interested parties. Lastly, the policy must be regularly reviewed and owner of the policy be defined.

2.6.5 Wireless Use Policy

Wireless policy specifies the conditions that should be met by the wireless infrastructure devices for them to be granted access. In an attempt to improving patients care, offering good patients experience hospitals cannot ignore success that comes with implementation of wireless network (Leibovitz, 2013). The large number of devices accessing wireless network in a hospital increases the attack surface thus a balance between giving access and security of the network should be balanced.

Wireless policy plays a significant role in ensuring that patient's information are secure against breach.

2.6.6 Backup Policy

Backup policy provides a framework for data backup process. The policy applies to data stored on organizations systems. The policy also dictates the type of data that should be backed up, frequency of backing up data, methods of backing up and who to access the data. In case of a disaster such as fire or floods the backed up data provides for the continuity of the business. Personal healthcare information for patients should also be backed up.

2.7 Models Informing the Study

The models discussed below informed the researcher in coming up with Cybersecurity Readiness Index model.

2.7.1 Cyber Readiness Index 2.0

Cyber Readiness Index 2.0 is a cyber readiness methodology developed by Potomac Institute for policy studies. This methodology ranks countries based on their cyber readiness. Almost all countries worldwide have embraced ICT in an effort to provide fast, affordable, and reliable communication. Initiatives such as e-banking, e-government, e-health, and e-learning are top economic agenda in most countries. The purpose of Cyber Readiness Index 2.0 is to inform leaders on what steps they should consider in protecting their increasingly connected countries and to evaluate a country maturity and commitment to cybersecurity in an effort to protect its vital infrastructure (Demchak, Kerben, McArdle & Spidalieri, 2015). The Cyber Readiness methodology takes into consideration seven unique elements; National strategy, E-crime and law enforcement, Information sharing, Investment on Research and Development, Incident response, Defence and crisis response and Diplomacy and trade (Demchak et al, 2015).

2.7.2 Cybersecurity Self-Assessment Tool

The Cyber Self-Assessment Tool was developed by Maryland Health care Commission to help small healthcare providers in checking Gaps in cybersecurity process. The tool was developed using the Cyber Security Framework (CSF) and National Institute of Standards and Technology (NIST) which are some of the commonly used Frameworks for evaluating cybersecurity.

The tool uses the Five core functions of NIST CSF; Identify, Protect, Detect, Respond, and Recover. The healthcare providers assesses their readiness by ticking from the four options the most appropriate option that reflects the organization's readiness. The Four options comprises of Informal, Developing, Established, or N/A.

2.7.3 SSH Hong Kong Enterprise Cyber Security Readiness Index

In line with Hong Kong Smart City vision which is meant to make use technology to address urban challenges. This vision is characterized by intensive network communication and use of big data. This will provide opportunities for attackers. This meant that every sector both private and public should be able to check their cyber readiness status.

The maturity of current security status is assessed in four aspects; process control, technology control, human awareness and security risk assessment. The range of index is from 0-100. The higher the number the ready the institution.

Table 2.1: SSH Hong Kong Enterprise Cyber Security Readiness Index

Index (0 – 100)	Level	Description
0 – 20	Unaware	The management at this level is not aware about necessary investment to be made cyber security This level is characterized by lack of policies and cyber security assessment to know the vulnerabilities
20.1 – 40	Ad-hoc	The organization begins to be aware of security investment Characterized by reactive, and inconsistent measures in reaction to attack
40.1 – 60	Basic	The awareness to protect the organization has been built and continuity is maintained. The level is characterized by some form of cyber security function. Technology controls is implemented but lacks centralized management. Awareness is provided but limited to only a few staff
60.1 – 80	Managed	The organization is aware to manage in a controlled way Characterized by organized fully cyber security function. Comprehensive cyber policy and the management is centralized. Awareness is provided to every single staff
> 80	Anticipated	Organization is able to anticipate cyber threats and comply with the requirements. Characterized by full support of management. Practice proactive defense. Organization aware of the global threat landscape and communicate it to the third parties

2.7.4 Global Cybersecurity Index (GCI)

Global Cybersecurity Index (GCI) was initiated by International Telecommunication Union (ITU). The questionnaire is deployed online and filled by 193 member states of ITU. The main purpose of GCI is to measure the member states commitment to cybersecurity with respect to five pillars; legal, technical, capacity building, and cooperation. The five pillars is divided in sub-pillars as shown in the figure 9.

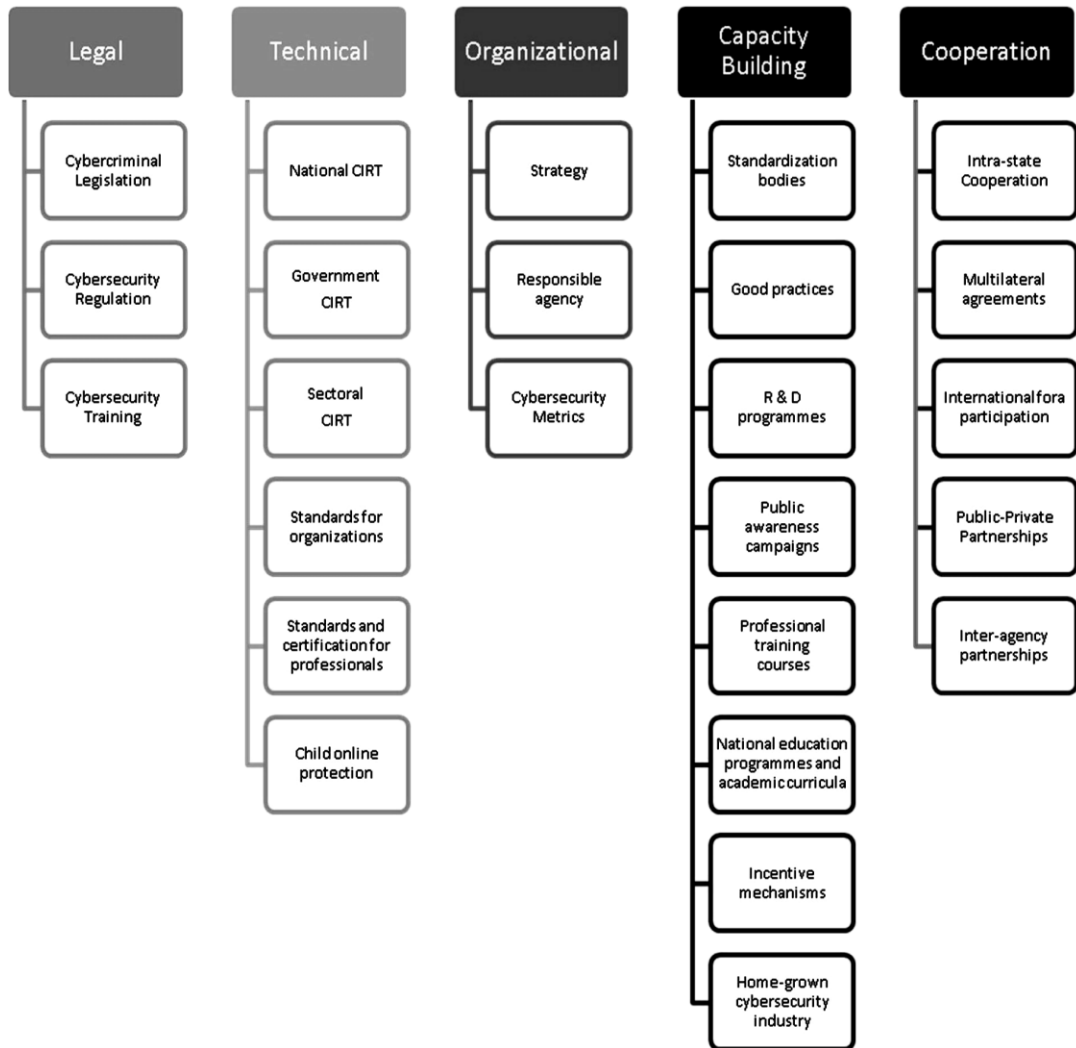


Figure 9: Pillars of GCI
Source: Brahim, S. (2017)

2.7.5 ISO/IEC 27001

ISO/IEC 27001 is an information management system (ISMS) standard published by ISO & IEC. This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within an organization. It specifies requirements for the implementation of information security controls customized to the needs of individual organizations or parts thereof. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. It is seen as an internationally recognized structured methodology

dedicated to information security management. ISO/IEC 27001 covers all types of organizations (private, government, non-profit making organization).

The standard introduces the “Plan-Do-Check-Act” (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization’s ISMS. The PDCA cycle has four phases: Plan – establishing the ISMS; Do – implementing and operating the ISMS; Check – monitoring and reviewing the ISMS; Act – maintaining and improving the ISMS.

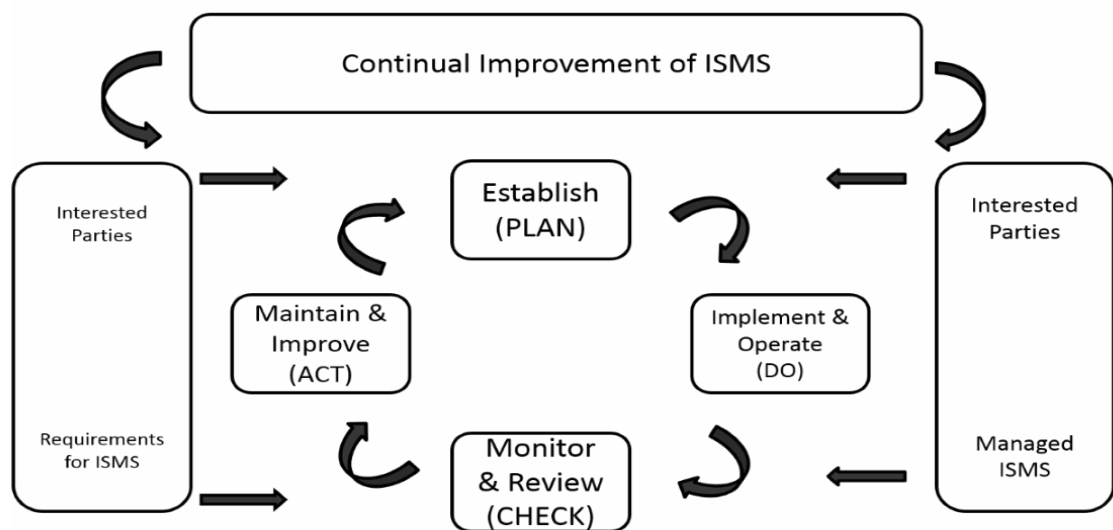


Figure 10: PDCA model
Source ISO/IEC (2005)

ISO/IEC 27001 does not dictate the exact information security controls since these controls vary distinctively across all organizations adopting the standard. ISO/IEC 27001 document mentions valuable details on information security risk that can be used as selection criteria for a proper information security risk assessment approach that builds upon the controls list proposed by the standard. These controls are grouped into fourteen control objectives namely; organization of information security, cryptography, human resource security, access control, asset management, physical and environment security, communication security, system acquisition development and maintenance, supplier relationship, information security incident management, operation security information security aspects of business continuity management, information security policies and compliance.

2.7.6 The Health Insurance Portability and Accountability Act (HIPAA)

The health insurance portability and accountability act (HIPAA) was constituted by the congress in the year 1996 and updated with HITECH act in 2009. Originally, HIPAA was meant to improve portability and accountability of health insurance coverage for employees between jobs, combat waste, abuse and fraud in healthcare sector. It was expanded cover security, privacy and breach notification. The privacy rule sets the standards for protected health information (PHI) for which it may be disclosed after use (Akowuah, 2012). Security rule specifies the safeguards that must be put in place in order to protect electronic protected health information (ePHI) for the confidentiality, integrity and availability to be maintained (Mohammed et al., 2015). Breach notification rule requires that the covered entity notify the affected individuals, the government and other case the media. HIPAA requires the technical, the administrative and the physical safeguards to secure the ePHI. Certain safeguards are considered required while others are addressable. Addressable safeguards does not mean it is optional but the covered entity may choose not to implement it if there valid reason which must be documented.

2.7.7 Health Information Trust Alliance (HITRUST)

The healthcare information trust alliance (HITRUST) was established with the sole purpose for promoting information security in healthcare sector while letting for the adoption of health information systems. HITRUST believes that security of information in healthcare sector is a critical step in provision of quality healthcare. Under the guidance of HITRUST multiple organizations came together to develop common security framework (CSF). CSF ids the only cybersecurity framework tailored to be used by healthcare.

2.7.8 Common Security Framework (CSF)

Common security framework was established in 2005 by the health information trust alliance (HITRUST) in conjunction with healthcare and information security specialist (Akowuah, 2012). CSF was developed to be used by organizations that create, access, and store and exchange health information. CSF is the first security framework tailored for healthcare sector. It leverages both existing standards (NIST, ISO) and regulatory standards such as HIPAA to avoid redundancy in healthcare industry (Akowuah, 2012). The framework is divided into two components;

information security control specification manual and standards and regulations mapping.

2.8 Research Gap

According to the reviewed literature, the researcher noted that very little had been done concerning the cyber readiness of healthcare sector. The cyber Readiness Index (2.0) was developed by Potomac institute of business studies, this readiness index measures a country preparedness and commitment to cybersecurity in its infrastructure. The only downfall to this methodology is that it focuses on country's infrastructure in general and does not narrow down to specific organizations such as the healthcare sector. Maryland healthcare commission has developed a tool called Cybersecurity Self-assessment Readiness tool to measure the cybersecurity readiness for hospitals. One has to fill the paper form and calculate the readiness manually, the tool also does not provide recommendations. Clearwater Compliance in conjunction with Intel are in the process of developing a model.

ISO 27001 and NIST cyber security framework have both laid the foundation but little has been done in healthcare sector has compared to other sectors such as the financial sector. This is attributed to the evolving nature of cyber-attacks. Few years ago attackers majorly focused on financial institutions such as banks but lately many hospitals have fallen victims of cyber-attack, this cyber shift is backed up by recent malware attack that wreaked havoc among hospitals. This study intends to fill the gap by designing a model for computing cyber security index as a web application by incorporating the 4 elements of cyber security in an organization, namely; people, processes, technology and policy. This assessment tool can be assessed online and also provide relevant recommendations thus solving the downfalls of the existing tools

2.9 Conceptual Framework

The conceptual framework that directed the research was presented in two stages; First stage showed the conceptual framework for derivation of formula for computing Cyber security Readiness index, and the second stages showed the architectural conceptual framework for implementation of the prototype. Figure 11 shows the conceptual framework for derivation of the formula

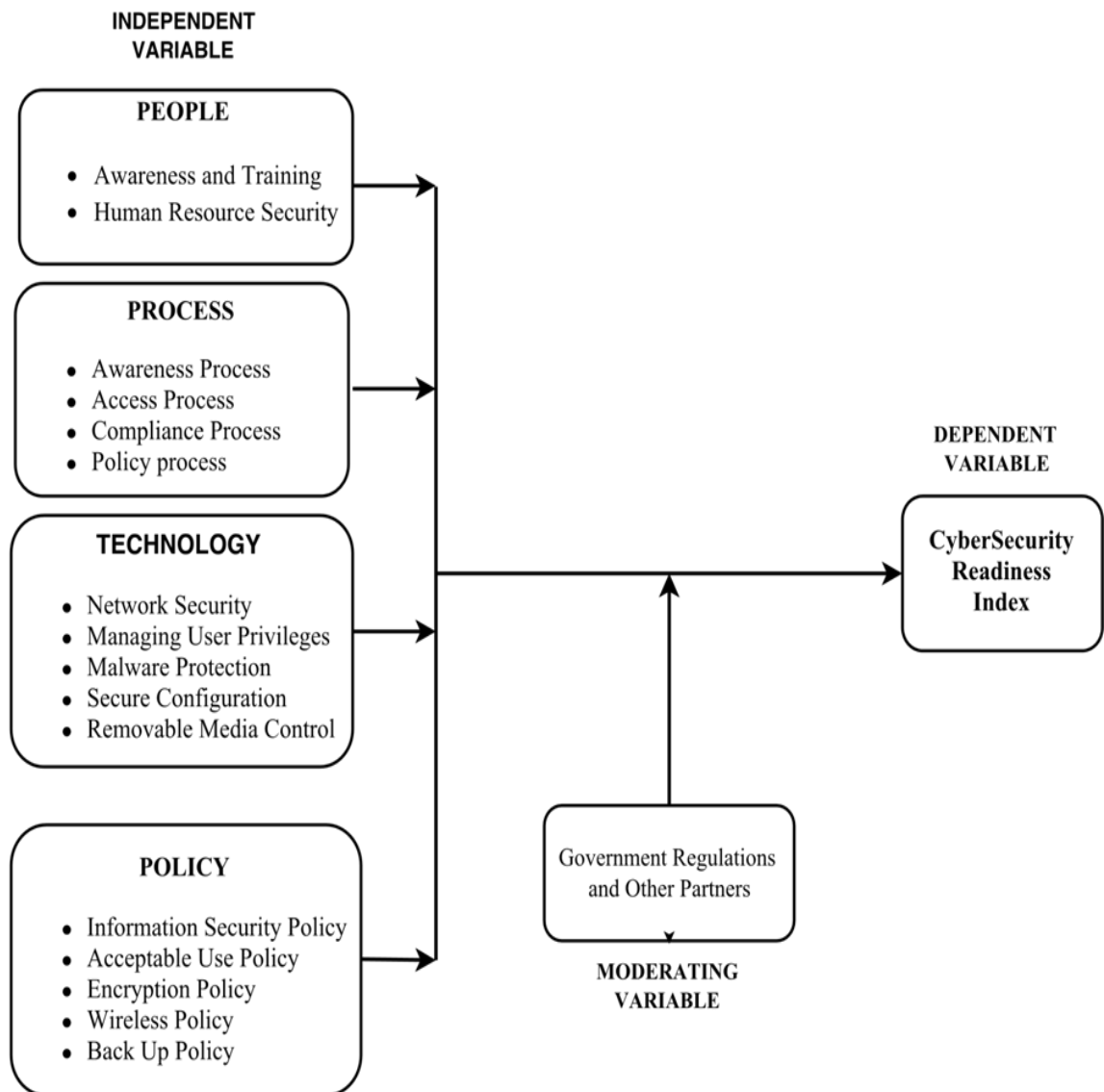


Figure 11: Conceptual framework
Source: Researcher (2018)

The second stage of the conceptual shows the architectural framework that will guide the development of the prototype

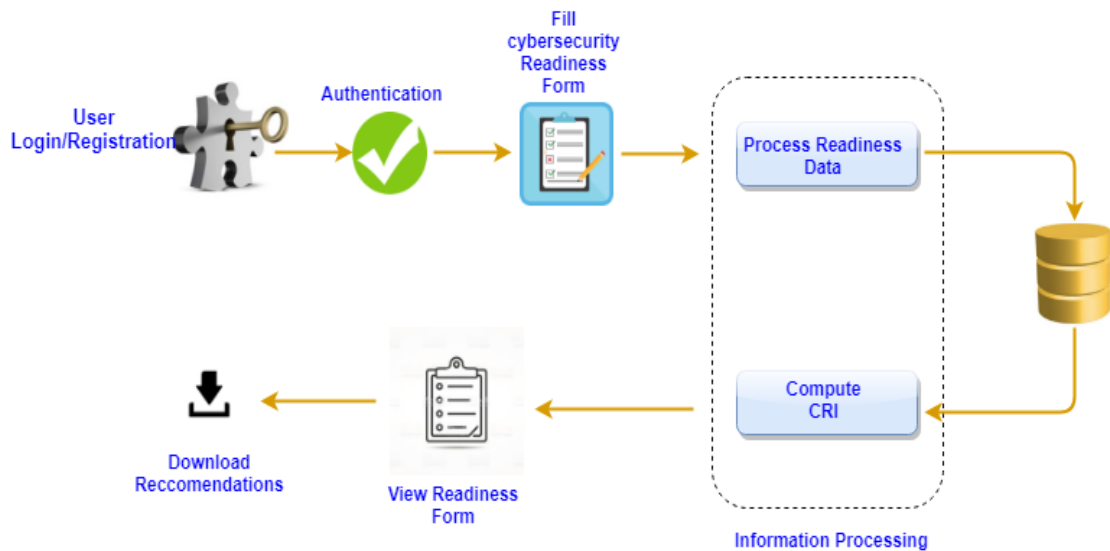


Figure 12: Architectural conceptual framework
Source: Researcher (2018)

The prototype has six modules; User Registration module, User login and authentication module which limits access to only authorized users, Readiness input module (digital questionnaire) that prompts the users to feed in Readiness information, Record management module for storing readiness information and weights, and information processing module to compute CRI from the stored weights and cyber security readiness information provided by the users. The prototype has a module to display CRI information and provide a mechanism for downloading CRI information and appropriate recommendations.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

Rajasekar, Philominathan, and Chinnathambi (2006) defines research methodology as the science of studying how research is undertaken. Essentially, the procedure by which researchers follow in an attempt to describe, explain and predict a phenomena. This chapter discusses the research design, the target population, sample, sample size, sampling techniques, data collection and analysis are also discussed. The chapter goes ahead to discuss the development, the implementation and the evaluation of the model. Finally, the ethical considerations is also outlined.

3.2 Research Design

A research design is a comprehensive outline of how a research will be conducted and involves description of such considerations as data collection methods, types of data collection instruments, and how collected data will be analysed. In view of the above, this research employed a quantitative research design. A quantitative research design is an orderly investigation of scientific mathematical properties and their relationships (Cooper & Schindler, 2011). Quantitative design also examines relationships between variables the objective of analysing and representing the relationship mathematically using statistical analysis. According to Mugenda and Mugenda (2003) quantitative approach focuses on technique, design, and measures to produce quantifiable or numerical discreet data. The quantitative method was used to gather the required data that was used by the researcher to develop the model

3.3 Location of the Study

This study focused on 11 hospitals both private and public operating within Nakuru County. Nakuru County was selected for the research due to a number of reasons; first, Nakuru has some of the best hospitals in the country and some of these hospitals are based on many parts of the country such as Mediheal, Karen Hospital, Nairobi Women Hospital and Agha ghan hospital, thus Nakuru is a representation of the whole country. Secondly, Nakuru is a cosmopolitan area and lastly, it was convenient to conduct research in Nakuru since the researcher is based in Nakuru.

3.4 Population of the Study

According to Ngechi (2004) a population is a well defined set of services, people events, elements or groups of things that are under investigation to generalize results. Statistics defines a target population as a specific group about which information is desired. The target population are human resource manager, ICT manager, system administrator, database administrator and Medical records manager. The 5 target population were selected based on the knowledge needed for the research.

3.5 Sampling Procedure and Sample Size

The study applied Purposive sampling. This type of sampling technique selects the sample based on the knowledge or experience of the sample group. Purpose sampling was employed in this study to select hospitals that have embraced ICT. 5 respondents namely; human resource manager, ICT manager, system administrator, database administrator, and Medical records manager from 11 selected hospitals both private and public were selected for the research.

3.6 Instrumentation

The study relied on the use of structured questionnaire to collect data. The questionnaires were designed based on the study objectives so as to provide relevant and in-depth information for the study. Each item is made to address specific theme of the study. The respondents were briefed on how to fill the questionnaire and given time to respond to the questionnaire after which it was collected. Questionnaires were selected for this study since one can collect voluminous data within a short time and also it is less costly.

3.6.1 Validity of the Instrument

An instrument is valid if it measures what is intended to measure and accurately achieve desired purpose it was designed for. According to Patten (2007) content validity is determined by judgement on the suitability of the instrument content. External validity is the extent at which the results can be generalized beyond the sample used for the study. It usually depends on the degree at which the sample represents the population. The validity of the questionnaire in this study was ensured by going through the questionnaire in relation to set objectives to ensure that it contains all necessary information that answers the objectives.

3.6.2 Reliability of the Instrument

Reliability is a measure of degree at which the selected instrument produces consistent data after repeated trials (Mugenda & Mugenda, 2003). The reliability of the instrument in this study was achieved through a test-retest procedure. Reliability was computed. A reliability of 0.642 for respondent's questionnaires was realized; hence the researcher considered the instrument reliable.

3.7 Data Collection Procedure

This study entirely employed primary data collection. The primary data was collected through the use of structured questionnaires which were administered on a drop-and-pick method. Questionnaires was chosen for this study because they are able to collect views and opinions of large number of respondents within a short time. The researcher personally distributed and collected the questionnaires upon completion for analysis. Both descriptive and inferential analysis methods were used for the analysis of results.

3.8 Model Development

The Cybersecurity Readiness Index (CRI) was computed as a function of weight assigned to cybersecurity elements and implemented as a mathematical model demonstrated by the formula shown below;

Equation 1: Model Equation

$$CRI = W_1 C_1^E + W_2 C_2^E + W_3 C_3^E + \dots + W_n C_n^E + e$$

Where;

$W_1, W_2, W_3 \dots W_n$ respectively are assigned weights

$C_1^E, C_2^E, C_3^E \dots C_n^E$ Respectively are cybersecurity elements associated with cybersecurity for which in this case are the sub- components of people, process, technology and policy

While; e represents the error term.

3.11 Ethical Considerations

This refers to moral standards that a researcher should uphold when conducting the study. The researcher will seek to assure the respondents that the study will entirely be used for academic purposes and nothing else. Respondent's participation will be on voluntary basis. Respondents will not be coerced into participating in the study but rather will have prior adequate information about the study from which they can choose to take part or not. Respondents will be assured that their privacy and confidentiality of their information will be protected by strict ethical standards of anonymity.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the general information of the organization under study, descriptive and quantitative analysis, correlations, regression analysis, and finally model implementation.

4.2 Response Rate

During data collection 55 respondents who were sampled through census method were issued with questionnaires which were collected when they were duly filled. It was noted that 50 of the questionnaires were returned which translated to a return rate of 91%. The collected questionnaires were therefore used for the study because they were considered to be enough for providing adequate results.

4.3 General Information

Classification of hospitals and position held were analysed in order to gain an understanding on their distributional pattern. Table 4.1 presents the findings.

4.3.1 Hospital Category

Categorizes hospitals into either private or public.

Table 4.1: Hospital Category

Category	Frequency	Percent
Public Hospital	18	36.0
Private Hospital	32	64.0
Total	50	100.0

According to analysed data, private hospitals were the majority with 64% while Public Hospital formed 36% of total population sampled.

4.3.2 Position

Shows the positions held by the research participants.

Table 4.2: Position Held

Position	Frequency	Percent
System administrator	5	10.0
Medical records manager	19	38.0
HR manager	8	16.0
Database administrator	3	6.0
ICT manager	15	30.0
Total	50	100.0

Out of 50 respondents, it was noted that Medical records managers constituted the largest percentage of 38%, followed by ICT managers at 30%, HR at 16%, system administrators at 10% and finally the database administrators constituted the least percentage with 6%.

4.4 Assessment of Cyber Security Readiness Elements

In order to attain objective one, the respondents were asked to give their opinion on criticality of the four cybersecurity elements. The responses are presented in Table 4.3

4.4.1 Cybersecurity elements Criticality

This section uncovers which Cyber security element is critical as per researched hospitals.

Table 4.3: Cybersecurity elements Criticality

Criticality	NVC (%)	NC(%)	N(%)	C(%)	VC(%)	χ^2	P
Criticality of Technology	6.0	10.0	18.0	36.0	30.0	16.40	0.003
Criticality of Policy	0.0	10.0	18.0	32.0	40.0	10.96	0.012
Criticality of Process	14.0	36.0	16.0	22.0	12.0	9.40	0.052
Criticality of People	22.0	32.0	10.0	12.0	24.0	8.20	0.085

Key: NVC-Not Very Critical; NC-Not Critical; N-Neutral; C-Critical; VC-Very Critical.

It was observed that policy was rated by 72% of responses as very critical significantly ($\chi^2=10.96$; $p<0.05$), and followed by Technology 66%. Similarly People and Process were rated to be critical at 36% respectively.

4.4.2 Descriptive Findings

This section presents the descriptive findings of each cyber security element with regard to cyber security. Chi-square test was used to determine whether the observed frequencies differed significantly from expected frequencies at 5% level of significance.

a) People: System user’s awareness with regard to cyber security

An assessment was done regarding system users awareness with regard to cybersecurity. Respondents were required to give their responses on whether they strongly agree, disagree, neutral, agree or strongly agree on the statements given. The findings are presented in Table 4.4

Table 4.4: System user’s awareness with regard to cyber security

Statement	SD	D	N	A	SA	χ^2	<i>p</i>
The mission, objectives and activities have been established and communicated to employee and third parties	6.0%	12.0%	12.0%	36.0%	34.0%	19.40	0.001
Cyber security awareness training and brown bag workshops are conducted to educate employee about phishing, identity theft, malware and spyware on annual basis	6.0%	22.0%	6.0%	44.0%	22.0%	24.40	0.000
Periodic review of employee system activity logs to inspect use, emails, file downloads and use of portable devices	0.0%	18.0%	16.0%	32.0%	34.0%	5.20	0.158
Policies and procedures have been defined and communicated to employee and third parties use of organization’s information technologies	6.0%	6.0%	12.0%	54.0%	22.0%	40.40	0.000
Employees and third parties to have access to information systems and software demonstrate understanding of their roles and responsibilities in protecting organizations physical systems and electronic access to information	0.0%	18.0%	16.0%	44.0%	22.0%	10.00	0.019
All senior management, employees and third parties have received training and demonstrate understanding of their roles in identifying, protecting, detecting, responding and recovering from cyber-attack	0.0%	24.0%	0.0%	34.0%	42.0%	2.44	0.295
Cybersecurity responsibilities and roles have been identified and communicated to employees including third parties	6.0%	12.0%	22.0%	42.0%	18.0%	18.80	0.001

Key:SD=Strongly Disagree, D=Disagree, N=Neutral, SA=Strongly Agree, A=Agree

It was distinguished that 18% of respondents disagreed that the mission, objectives and activities have been established and communicated to employee and third parties leaving 82% agreeing. In addition, 30% disagrees that cyber security awareness training and brown bag workshops are conducted to educate employee about phishing, identity theft, malware and spyware on annual basis. This implies that the cyber security is a big challenge in hospitals sampled. On the other hand, only 34% maintains that periodic review of employee system activity logs to inspect use, emails, and file downloads and use of portable devices and that policies and procedures have been defined and communicated to employee and third parties use of organization's information technologies (76%). However, their, responses did not differed significantly ($\chi^2=15.20$; $p>0.05$). It was worth noting that 66% observe that employees and third parties to have access to information systems and software demonstrate understanding of their roles and responsibilities in protecting organizations physical systems and electronic access to information. As regards to training, 24% disagrees that all senior management, employees and third parties have received training and demonstrate understanding of their roles in identifying, protecting, detecting, responding and recovering from cyber-attack. Nonetheless, their responses did not differed significantly ($\chi^2=15.20$; $p>0.05$). Finally, this observation was echoed by 18% who reports that Cybersecurity responsibilities and roles have not been identified and communicated to employees including third parties.

b) Process: Laid Down Procedures of Operation for Monitoring Cybersecurity

An assessment was done regarding laid down Procedures of operation for monitoring cybersecurity. Respondents were required to give their responses on whether they strongly agree, disagree, neutral, agree or strongly agree on the statements given. The findings are presented in Table 4.5

Table 4.5: Procedures of Operation for Monitoring Cybersecurity

Statement	SD	D	N	A	SA	χ^2	<i>p</i>
The environment outside of IT systems is monitored for unauthorized access	6.0%	12.0%	22.0%	34.0%	26.0%	12.40	0.015
All cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat	16.0%	24.0%	18.0%	26.0%	16.0%	2.20	0.699
All cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat	4.0%	34.0%	24.0%	20.0%	18.0%	11.80	0.019
The organization has identified and prioritized all activities essential for its' operation	0.0%	20.0%	18.0%	34.0%	28.0%	3.28	0.350
All roles and responsibilities for managing cybersecurity processes are coordinated to avoid duplication and are aligned to the employees position	0.0%	16.0%	20.0%	24.0%	40.0%	6.64	0.084
The organization has identified and documented known cybersecurity threats and the potential impact of unauthorized access to information and used this information to determine organization's level	0.0%	22.0%	18.0%	28.0%	32.0%	2.32	0.509
The organization has mapped how information and data moves through the organization	0.0%	10.0%	0.0%	46.0%	44.0%	12.28	0.002

Key:SD=Strongly Disagree, D=Disagree, N=Neutral, SA=Strongly Agree, A=Agree

It was recognized from analysed data that 90% asserted that the organization has mapped how information and data moves through the organization. However, 40% disagrees that all cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat. Additionally, up to 38% reported that all cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat and that the organization has identified and prioritized all activities essential for its' operation(62%). On the other hand respondents disagreed that all roles and responsibilities for managing cybersecurity processes are coordinated to avoid duplication and are aligned to the

employees' position and that the organization has identified and documented known cybersecurity threats and the potential impact of unauthorized access to information and used this information to determine organization's level with 16% and 22% respectively.

c) Policy: Adoption of Cyber Security Policy

An assessment was done regarding adoption of cybersecurity policy. Respondents were required to give their responses on whether they strongly agree, disagree, neutral, agree or strongly agree on the statements given. The findings are presented in Table 4.6

Table 4.6: Adoption of Cyber Security Policy

Statement	SD	D	N	A	SA	χ^2	<i>p</i>
All users and devices undergo a standard approval process prior to use and their system identities and credentials are managed by designated authorized personnel	10.0%	16.0%	0.0%	34.0%	40.0%	12.24	0.007
Cybersecurity policies are continuously tested to determine their usefulness against new and emerging threats and how well they comply with industry best practices, which are continuously improved through incorporation of lessons learned	0.0%	16.0%	26.0%	40.0%	18.0%	7.12	0.068
Remote access is managed through formal approval and credentialing based on the role of the employee or third-party	0.0%	12.0%	14.0%	34.0%	40.0%	11.92	0.008
Personnel understand the legal and regulatory requirements governing Cybersecurity	10.0%	12.0%	24.0%	44.0%	10.0%	21.40	0.000

Permissions for users, devices, and software access to organization IT systems, equipment, and files is limited to only what is necessary to perform job functions or ensure normal functioning	0.0%	16.0%	6.0%	28.0%	50.0%	21.52	0.000
IT systems and data removal, transfer, storage, and destruction is standard throughout the organization	0.0%	14.0%	0.0%	48.0%	38.0%	9.16	0.010
Access to areas outside of the IT system is restricted, especially in areas where computers, devices, and files that contain sensitive information are kept	6.0%	10.0%	16.0%	40.0%	28.0%	19.40	0.001

Key:SD=Strongly Disagree, D=Disagree, N=Neutral, SA=Strongly Agree,

A=Agree

It was clear from finding that respondents significantly ($\chi^2=12.24$; $p<0.05$) agreed that all users and devices undergo a standard approval process prior to use and their system identities and credentials are managed by designated authorized personnel and also that remote access is managed through formal approval and credentialing based on the role of the employee or third-party with 74% respectively. Regarding Cyber security policies, it was reported by 58% that they are continuously tested to determine their usefulness against new and emerging threats and how well they comply with industry best practices, which are continuously improved through incorporation of lessons learned. Additionally, 54% observed that personnel understand the legal and regulatory requirements governing Cybersecurity. However, 16% disagreed that permissions for users, devices, and software access to organization IT systems, equipment, and files is limited to only what is necessary to perform job functions or ensure normal functioning. It was also shared by 14% who decried that IT systems and data removal, transfer, storage, and destruction is not standard throughout the organization. Finally, 68% acknowledged that access to areas outside of the IT system is restricted, especially in areas where computers, devices, and files that contain sensitive information are kept.

d) Information Technology: Safeguard of IT Systems against Cyber Attacks

An assessment was done regarding safeguard of IT systems against cyber attacks. Respondents were required to give their responses on whether they strongly agree, disagree, neutral, agree or strongly agree on the statements given. The findings are presented in Table 4.7

Table 4.7: Safeguard of IT Systems Against Cyber Attacks

Statement	SD	D	N	A	SA	χ^2	<i>p</i>
Consistent procedures for development and acquisition of IT systems and software are used	0.0%	4.0%	0.0%	50.0%	46.0%	19.48	0.000
Network penetration testing is conducted on an annual basis	8.0%	22.0%	12.0%	6.0%	52.0%	35.80	0.000
IT systems are protected by limiting changes to the system, software installation, connection of external devices, monitoring electronic communications, and users of the system	0.0%	4.0%	14.0%	58.0%	24.0%	33.04	0.000
All IT systems, software, and data is scanned to identify who sent it and/or where it came from, and assess how likely the source is to be reputable	0.0%	6.0%	30.0%	26.0%	38.0%	11.12	0.011
All information and data that is stored, transmitted, or accessed by the organization is protected from unauthorized access	0.0%	6.0%	0.0%	38.0%	56.0%	19.24	0.000
The IT systems, the network, software, and third party activity is monitored and scanned to detect malicious and unauthorized code, and identify unauthorized access	6.0%	14.0%	12.0%	40.0%	28.0%	19.00	0.001

Key: SD=Strongly Disagree, D=Disagree, N=Neutral, SA=Strongly Agree, A=Agree

As regards to technology, respondents asserted significantly that the IT systems, the network, software, and third party activity is monitored and scanned to detect

malicious and unauthorized code, and identify unauthorized access and that all information and data that is stored, transmitted, or accessed by the organization is protected from unauthorized access with ($\chi^2=19.00$; $p<0.05$); 68% and ($\chi^2=19.24$; $p<0.05$); 94% responses respectively. Similarly, 96% agreed that consistent procedures for development and acquisition of IT systems and software are used as 64% acknowledge that all IT systems, software, and data is scanned to identify who sent it and/or where it came from, and assess how likely the source is to be reputable. However, close to 18% disagreed that IT systems are protected by limiting changes to the system, software installation, connection of external devices, monitoring electronic communications, and users of the system. This was observed by 44% who disagreed that network penetration testing is conducted on an annual basis. On the basis of this observation, it necessitated this study to determine cyber security readiness index for hospitals towards adoption of e-health.

4.5 Cyber Security Readiness Model design

Table 4.8: Spearman's Rho Correlations

		Cyber Security Readiness
Cyber Security Readiness	Spearman's Rho Correlation Coefficient	1.000
	Sig. (2-Tailed)	.
	N	50
People	Spearman's Rho Correlation Coefficient	.712**
	Sig. (2-Tailed)	.000
	N	50
Process	Spearman's Rho Correlation Coefficient	.571**
	Sig. (2-Tailed)	.000
	N	50
Policy	Spearman's Rho Correlation Coefficient	.536**
	Sig. (2-Tailed)	.000
	N	50
Technology	Spearman's Rho Correlation Coefficient	.560**
	Sig. (2-Tailed)	.000
	N	50

** . Correlation Is Significant at the 0.01 Level (2-Tailed).

4.5.1 Correlation between System User's Awareness against Cyber Security Readiness

In determining whether there existed a relationship between cyber security readiness and the system users' awareness, Spearman's rho Correlation was conducted. It was noted that there existed a positive and statistically significant correlation between cyber security readiness and the system users awareness ($r=0.712^{**}$; $p<.0.01$). This implies that when system user's awareness is improved, the hospitals cyber security readiness index consequently increases and vice versa.

4.5.2 Correlation between the Laid Down Procedures of Operation for Monitoring Cybersecurity against the Cyber Security Readiness

In determining whether there existed a relationship between cyber security readiness and the laid down procedures of operation for monitoring cybersecurity, spearman's rho correlation was conducted. It was noted that there existed a positive and statistically significant correlation between Cyber Security Readiness and the laid down procedures of operation for monitoring cybersecurity ($r=0.571^{**}$; $p<.0.01$). This implies that when the laid down procedures of operation for monitoring cybersecurity is improved the hospital's cybersecurity readiness index increases and the opposite is true.

4.5.3 Correlation between the Adoption of Cyber Security Policy and Cyber Security Readiness

In determining whether there existed a relationship between cyber security readiness and adoption of cyber security policy, spearman's rho correlation was conducted. It was noted that there existed a positive and statistically significant correlation between cyber security Readiness and Policy ($r=0.536^{**}$; $p<.0.01$). This implies that once the adoption of cyber security policy is implemented the hospital's cyber security readiness index is increased. Conversely, lack of implementation of adoption of cyber security policy reduces the hospital's cyber safety

4.5.4 Correlations between IT Safeguards and Cyber Security Readiness

In determining whether there existed a relationship between cyber security readiness and the IT safeguards, spearman's rho correlation was conducted.

It was noted that there existed a positive and statistically significant correlation between cyber security readiness and the IT safeguards ($r=0.560^{**}$; $p<.0.01$). This implies that when the information technology safeguards are put in place the

hospital's cyber Security readiness is increased. However, absence information technology safeguards reduces hospital's cyber security readiness.

4.6 Regression Analysis

Regression was conducted in order to predict statistically the dependent variable using independent variable. It should be noted that the regression equation formed the primary equation for the model to be developed.

4.6.1 Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.892 ^a	0.796	0.778	0.33

a. Predictors: (Constant), Technology, People , Policy, Process

Model summary in Table xx shows Adjusted R Square value of as 0.778 indicating that. 77.8% of variation in cyber security readiness is explained in the variation of independent variables with a standard error of the estimate of 0.33.

4.6.2 Anova Statistics

F-statistics were computed find out the overall significance of the model

Anova^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	18.902	4	4.725	43.862	.000 ^b
	Residual	4.848	45	.108		
	Total	23.750	49			

A. Dependent Variable: Cyber Security Readiness

B. Predictors: (Constant), Technology, People , Policy, Process

The findings indicates that the model is significant at 95% confidence level; $R^2 = 0.796$, $F(4, 45) = 43.862$; $p < 0.05$. This indicates that the model is efficient in predicting the effect of independent variables on dependent variable.

4.6.3 Regression Coefficients

Coefficients^a

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.230	.325		0.709	.482
People	.516	.058	.669	8.830	.000
Process	.012	.082	.012	0.145	.886
Policy	.285	.059	.370	4.861	.000
Technology	.090	.091	.083	0.987	.329

a. Dependent Variable: Cyber Security Readiness

4.7 Derivation of Relevant Weight for CRI Mathematical Model

To get the cybersecurity readiness index (CRI) of a hospital, readiness assessment questions were asked in the form of a Likert scale of 1 to 5. 1 meant that the respondent strongly disagree with the readiness statement while 5 meant that the respondent strongly agree with the statement. Other options included; Disagree, Neutral and Agree.

The score per assessment question denotes the level of readiness of a hospital with regard to the four elements affecting cybersecurity. Multiple linear regression model equation was used to derive relevant weights. These weights were relevant in deriving the cybersecurity readiness index (CRI).

Equation 2: Multiple regression

$$Y = C + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + e$$

Y = Dependent Variable (Cybersecurity Readiness Index)

C = Intercept (Constant)

β1 = Predictable Variable coefficients (Weights)

X1, X2, X3, X4 = Independent Variables (people, process, policy and technology respectively)

e = Error term

Given the equation;

$$\text{CRI} = 0.230 + [0.516 * \text{People}] + [0.012 * \text{Process}] + [0.285 * \text{Policy}] + [0.090 * \text{Technology}] + 0.33$$

4.8 Model Scenarios

This section discusses the four possible scenarios namely; Best-case scenario, Average-case scenario, and worst-case scenario.

4.8.1 Best Case Scenario

Best-case scenario is achieved when a user scores an average score of 5 in each assessment question amounting to 35 for all questions since each category has 7 questions.

Equation 3: Best case scenario

$$\text{CRI} = (C + e + (0.516 * \text{people}) + (0.012 * \text{Process}) + (0.285 * \text{Policy}) + (0.090 * \text{Technology})) * 100 / \text{Max score}$$

$$\text{CRI} = ((0.230 + 0.33 + (0.516 * 35) + (0.012 * 35) + (0.285 * 35) + (0.090 * 35)) * 100) / 32.165 = 100\%$$

4.8.2 Average Case Scenario

The average case scenario is the middle position where a hospital is neither exposed to cyberattacks or ready to fight cyberattacks. The average case scenario is achieved when an assessee scores an average of 2.5 per assessment question. This amounts to 17.5 for each variable category

Equation 4: Average case scenario

$$\text{CRI} = (C + e + (0.516 * \text{people}) + (0.012 * \text{Process}) + (0.285 * \text{Policy}) + (0.090 * \text{Technology})) * 100 / \text{Max score}$$

$$\text{CRI} = ((0.230 + 0.33 + (0.516 * 17.5) + (0.012 * 17.5) + (0.285 * 17.5) + (0.090 * 17.5)) * 100) / 32.165 = \sim 50\%$$

4.8.3 Worst Case Scenario

The worst case scenario is the position where a hospital is fully exposed to cyberattacks. Worst case scenario is reached at when an assessee scores an average of 1 for each assessment question. This adds up to 7 for each variable category since there are 7 questions for each variable.

Equation 5: Worst case scenario

$$CRI = (C + e + (0.516 * \text{people}) + (0.012 * \text{Process}) + (0.285 * \text{Policy}) + (0.090 * \text{Technology})) * 100 / \text{Max score}$$

$$CRI = ((0.230 + 0.33 + (0.516 * 7) + (0.012 * 7) + (0.285 * 7) + (0.090 * 7)) * 100) / 32.165 = \sim 21\%$$

4.9 Threshold Scores and assessment scale

According to CRI model, the score was set in a score of 1 to 5. The threshold score was pegged at 4. This score denotes that assessee agrees with the cybersecurity assessment questions. Score of 5 denotes that the assessee agrees strongly with the cybersecurity assessment questions. This also implies that hospital is ready to fight cyberattacks. However, a score of 1, 2 and 3 is below the threshold score (4) means that the hospital is at a high risk of being attacked. The score below threshold calls for stunt actions to be taken to secure the hospital thus recommendations are pegged at this score

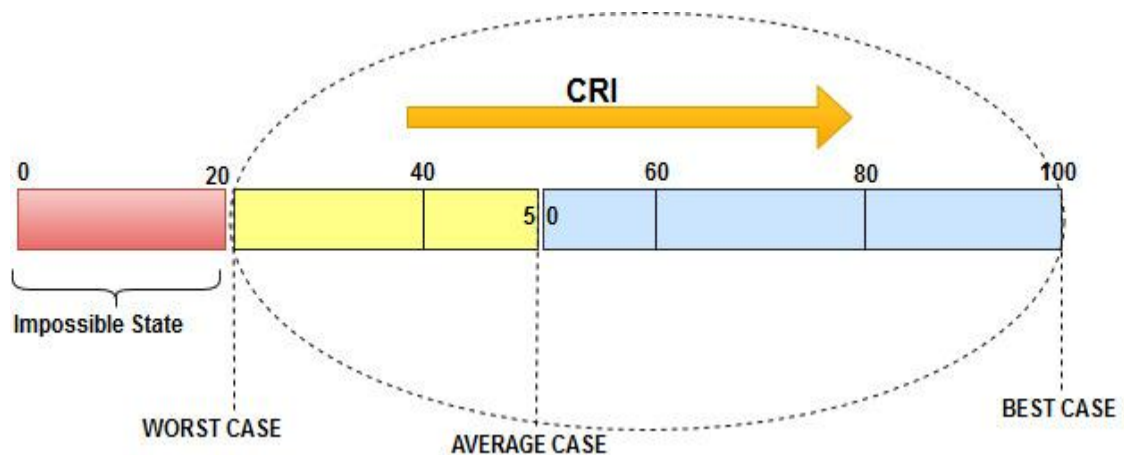


Figure 14: Assessment Scale
Source: Researcher (2018)

As demonstrated in equations above, the worst case scenario, average case scenario and best case scenario is represented by 21%, 50% and 100% respectively. The 0% readiness cannot be computed from the model due to two reasons. First one is because of error term and the second one is because the model computation for these factors is pegged on a scale of 1 to 5, which yields the said results. This is called the impossible state.

4.10 Model Implementation

Model implementation provides comprehensive discussion on entire process that was followed in implementation of cybersecurity readiness index (CRI) model as a prototype. As a proof of concept, the SREI system prototype was developed using PHP as a server side scripting language for system logic controllers. Front end scripting was done using JQuery library to enhance front end responsiveness to the platform while styling was done using Bootstrap. PHP storm editor was used to write and test code. Apache web server was used to run the application locally and MySQL was used as backend database engine. The system was hosted online after development and can be accessed through the URL: <http://matricuda.com/limomodel/index.php>

4.10.1 CRI System Design

This section provides the overall platform overview beginning with the system objectives, functional overview, and process of achieving CRI system functionality, system architecture and interface.

4.10.2 System Objective

The core objective of this study was to design a web –based model that would enable hospitals perform their independent assessment to determine their cybersecurity readiness index (CRI). CRI informs hospitals of how ready they in averting the cyber-attack by focusing on the four elements cybersecurity elements; people, process, technology and policy. The platform also provides recommendations on what needs to be done in order to increase the hospitals cyber readiness.

4.10.3 System Function Overview

In the process of developing cybersecurity readiness model for hospitals to perform independent assessment, different types of technologies were implemented. CRI platform was developed using PHP as the server side scripting language, MySQL as the database engine, JQuery for interactive functions and CSS3 for styling. Security is the core of any web model. Security was enforced in the model to ensure that users are authenticated before running any assessment, viewing assessment information and accessing any model functionalities. All users were needed to register by providing their names, name of the organization, email address and password.

4.10.4 Processes to Complete SREI System functionality

Rapid prototyping model was used as system development method for CRI system as discussed in section 3.3. The process below was followed.

- a) **Requirement gathering process:** The requirements for the development of CRI model was gathered from cyber readiness depicted by the hospitals and the escalating threat landscape reviewed in the literature review
- b) **Quick design process:** A quick conceptual design of the CRI system and its modules was done using the flow diagram shown below.

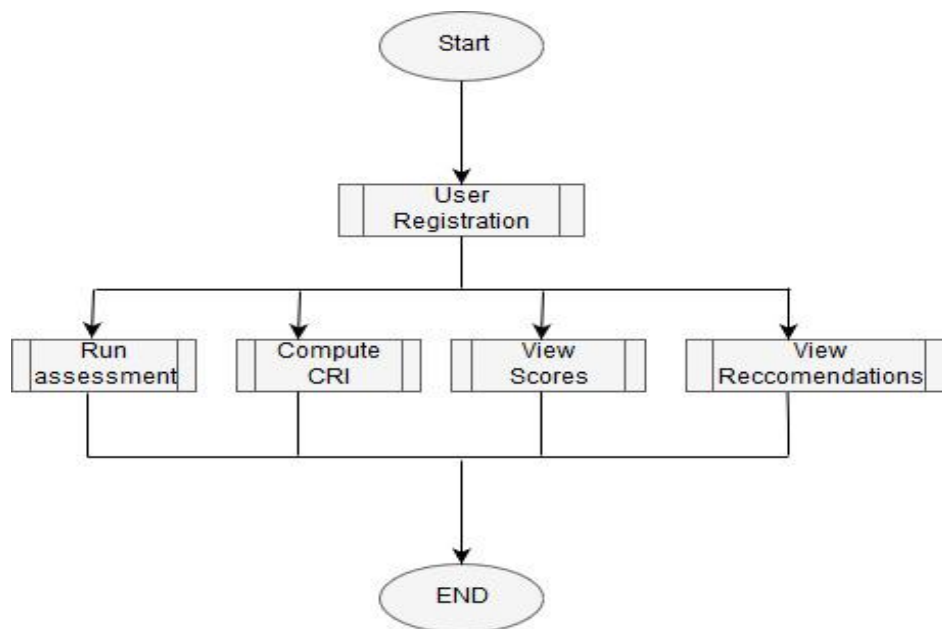


Figure 15: CRI system flow chart
Source: Researcher (2018)

- c) **Prototype Design Process:** CRI platform was developed using PHP as the server side scripting language, MySQL as the database engine, JQuery for interactive functions and CSS3 for styling.
- d) **Evaluation Process:** The prototype was evaluated using IT-systems as such goal based, Heuristic evaluation, and Cognitive walkthrough.
- e) **Coding and Testing Process:** Upon the achievement of satisfactory requirements the code was refined. The final prototype was deployed online and users were allowed to register and login to test the system functionalities. Feedback form the users informed some further improvement on the system.

- f) **Deployment process:** After addressing the users concerns raised on the testing process, the complete system was deployed online.

4.10.4 CRI System Architecture

This section presents the entity relationship diagram for the CRI and the different modules that make up the system.

1. Entity Relationship Diagram (ERD)

The entity relationship diagram for the CRI system is as shown in Figure 16. It contains 4 database tables for storing four main types of information;

- User registration and authentication information: user_id, username, email, organization, and password (MD5 cryptographic hash)
- System Questions information: question_id, category, questions, category_weight, recommendations, threshold.
- User Assessment: User_id, questions_id, score, assessment_date, questions.

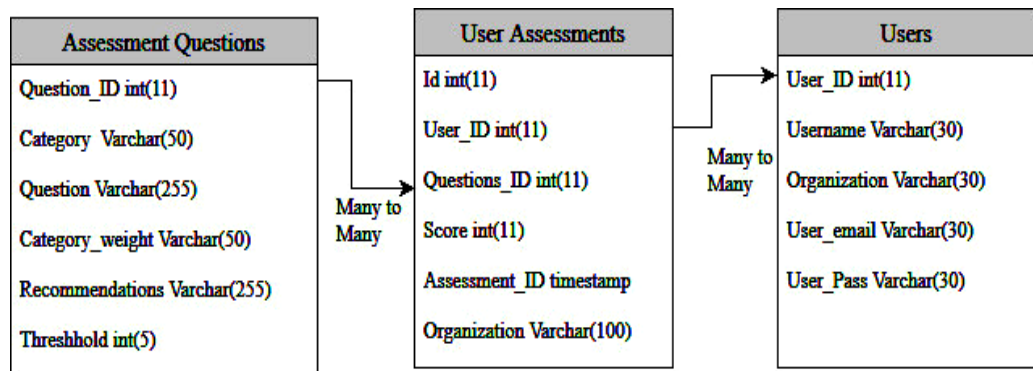


Figure 16: Entity Relationship Diagram
Source: Researcher (2018)

- User authentication module:** This module ensures that only the registered users who have permission to access the functionality are allowed are allowed to do so while others are denied access, this creates a security context.
- User registration module:** This module is the first stage before a user is granted access to login to the system. The user registers by providing information such as user's full name, organization's name, email address and password.
- User login Module:** This module only allows registered users to access the system's functionality by providing the email and password. Both the email and

the password should match the ones provided during registration so as to be granted access.

- d) **Password management module:** This module handles password verification. It is also responsible for encryption of user's passwords in the database using SHA-256 algorithm
- e) **User Session Handling Module:** This module manages user sessions by creating a session when user logs into the system, track all the user activities when the session is on, and destroys the session when the user logs out of the system.
- f) **Readiness Assessment module:** This session pulls the readiness questions from the database and present it on a likert scale layout. The user goes through the questions and checks the appropriate answer depending on their organization's cyber readiness. After all the questions have been duly filled the user submits it.
- g) **Results module:** This module presents the results of the submitted assessment to the user in a graphical display. The user can also download the assessment results and recommendations in the form of portable document format (pdf).
- h) **Help Module:** This module provides help to the new users on how to navigate through the system.
- i) **Core application logic:** This module contains logic that handles user requests by receiving, processes, and responding to them. Moreover, this module allows inputs to the database, performs arithmetic computations of the cyber readiness index.
- j) **System Databases:** The CRI platform maintained by four database tables, namely; (i) users table that stores records of all registered users and acts as a reference by the authentication module on whether to allow user access or not, (ii) assessment questions table that stores a record as questions to be used for assessment, threshold scores per question, and corresponding recommendations, (iii) question categories table that stores a question categories depending on ISO27001 control clauses, and (iv) the user assessment table that keeps a record of assessments done by the user and appends a timestamp to each assessment submitted successfully. This is the most active table in the SREI system. The database design is discussed in section 5.2.5

4.10.6 System Design

This section presents the logical design of the CRI model

1. System Navigation

The CRI is a web-based application and therefore accessible through the use of web browser. CRI system interface communicates with the system components through the use of navigation links.

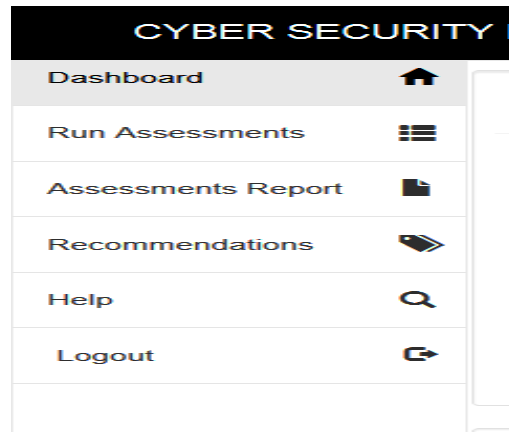


Figure 17: CRI system Navigation Panel
Source: Researcher (2018)

2. User Registration

This module is the first stage before a user is granted access to login to the CRI system. The user registers by providing information such as user's full name, organization's name, email address and password. After the user has provided the necessary required information, the details are stored in the database to be used by the login and authentication module. Figure 18 presents the flowchart for the registration module while Figure 19 shows the graphical interface of the same module.

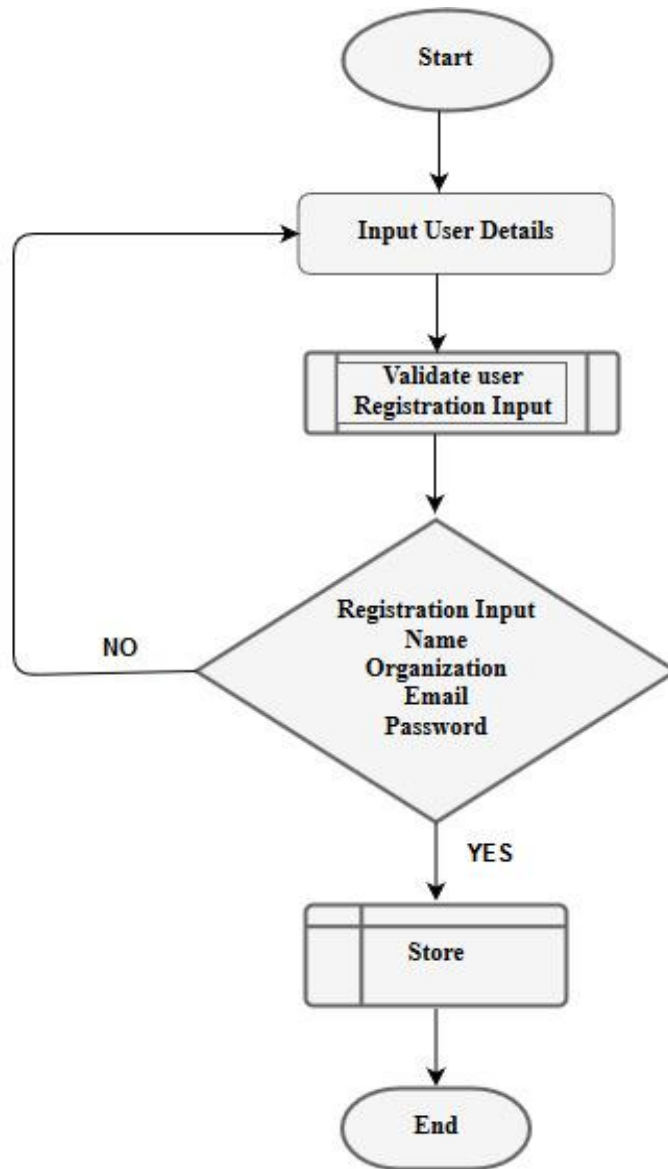


Figure 18: Registration Process Flowchart
Source: Researcher (2018)

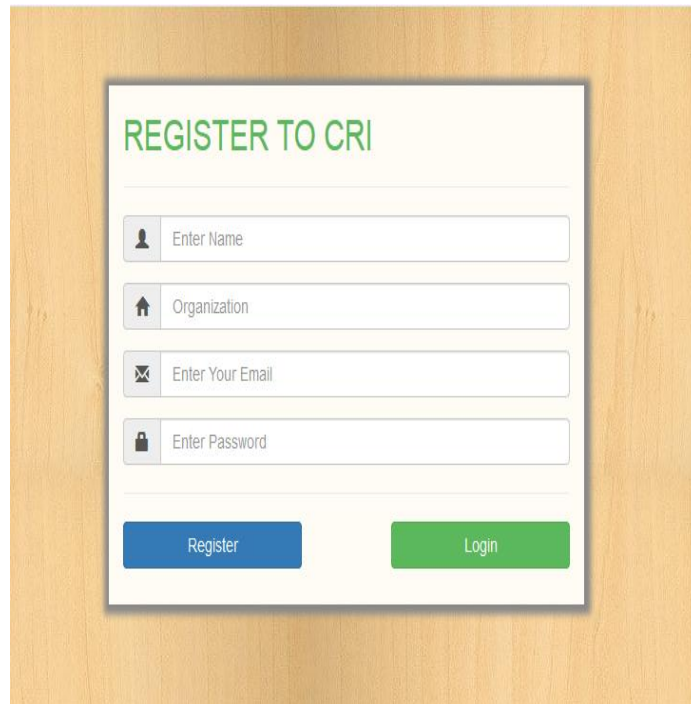


Figure 19: Registration GUI
Source: Researcher (2018)

3. Login Module

This module manages logins and sessions on users. It allows users who have registered to login into the systems functionalities. If the user is not registered the module denies them access by prompting them to enter the email and the password. Figure 20 below presents a flowchart for login logic module whereas Figure 21 shows graphical user interface of the login system.

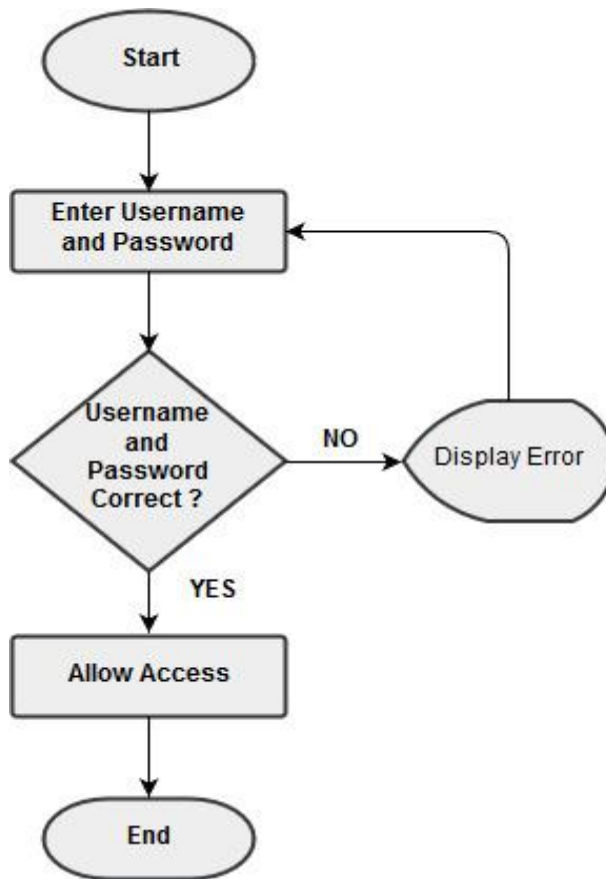


Figure 20: Login Process Flowchart
Source: Researcher (2018)

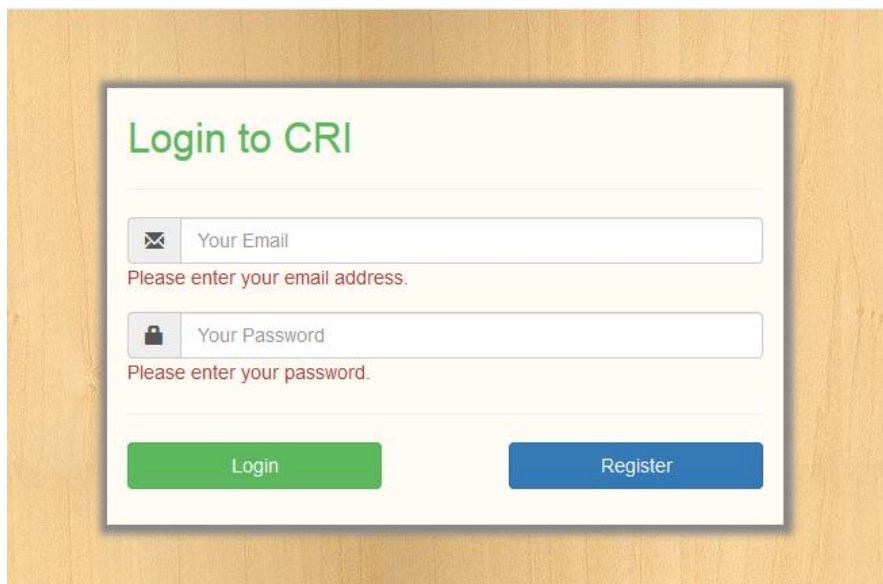


Figure 21: Login GUI
Source: Researcher (2018)

4. Readiness assessment Module

The readiness assessment module enables the user to perform self-assessment for their organization by selecting the radio button in respective assessment questions. The module pulls the assessment questions from the database and present it in a Likert layout. After dully filling the form, it is submitted back to the database for the computation of cybersecurity readiness index (CRI). The Figure 22 below presents a flowchart for the assessment logic whereas Figure 23 shows the graphical user interface for readiness assessment module.

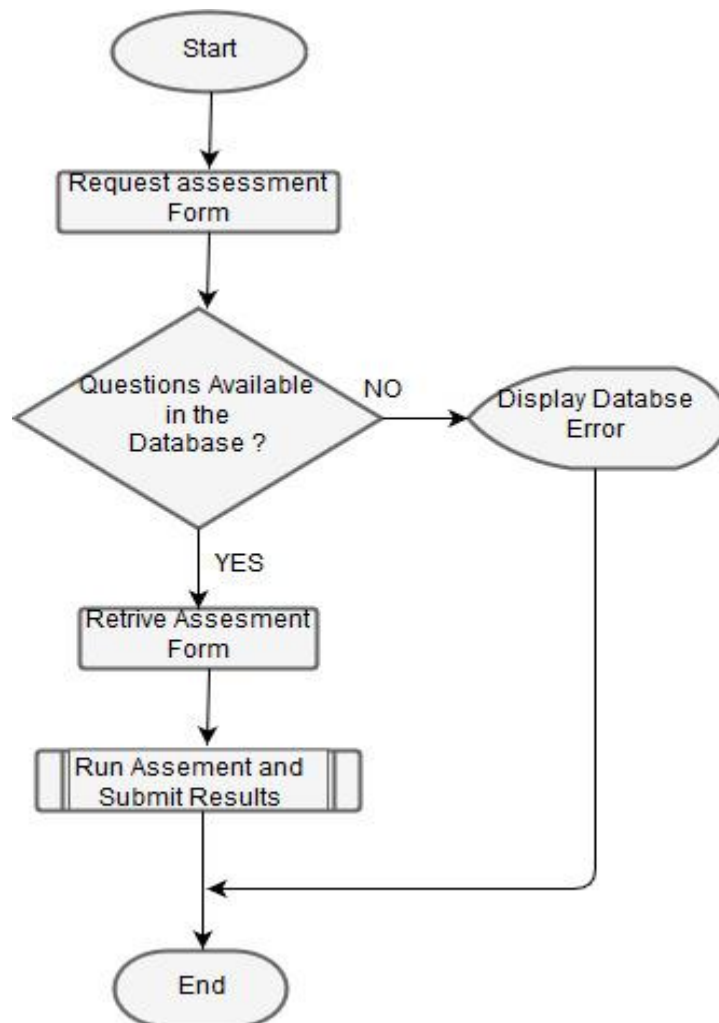


Figure 22: Readiness Assessment Flowchart
Source: Researcher (2018)

<p>INSTRUCTIONS: Please Fill in the Assessment Questions by Checking each radion button that best suits your organization. (KEY: 1=Strongly Disagree, 2=Disagree,3=Neutral, 4=Agree, 5=Strongly Agree)</p>							
NO	Category	Questions	1	2	3	4	5
1	People	Cybersecurity responsibilities and roles have been identified and communicated to employees including third parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	People	All senior management, employees and third parties have received training and demonstrate understanding of their roles in identifying, protecting, detecting, responding and recovering from cyberattack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	People	Employees and third parties who have access to information systems and software demonstrate understanding of their roles and responsibilities in protecting organizations physical systems and electronic access to information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	People	Policies and procedures have been defined and communicated to employee and third parties use of organization's information technologies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	People	Periodic review of employee system activity logs to inspect use, emails, file downloads and use of portable devices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	People	Cyber security awareness training and brown bag workshops are conducted to educate employee about phishing, identity theft, malware and spyware on annual basis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	People	The mission, objectives and activities have been established and communicated to employee and third parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	Process	The organization has mapped how information and data moves through the organization	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	Process	The organization has identified and documented known cybersecurity threats and the potential impact of unauthorized access to information and used this information to determine organization's level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	Process	All roles and responsibilities for managing cybersecurity processes are coordinated to avoid duplication and are aligned to the	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 23: Risk Assessment GUI
Source: Researcher (2018)

5. Assessment Scores Module

The assessment scores module allows users to view the assessment scores for all the questions submitted during assessment. The module also allows the user to download the assessment scores in form of a portable document format (PDF). Figure 24 shows the assessment score retrieval logic in a flowchart whereas Figure 25 shows the graphical user interface presentation of the module.

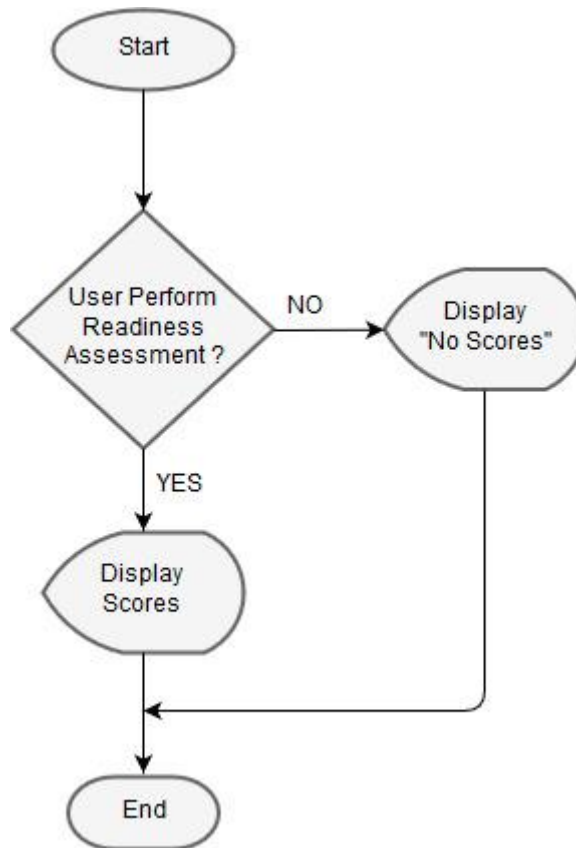


Figure 24: Score Flowchart
Source: Researcher (2018)

🔔 YOUR SCORES

QId	Question	Score	Recommendation
1	Cybersecurity responsibilities and roles have been identified and communicated to employees including third parties	1	2018-05-22 13:34:05
2	All senior management, employees and third parties have received training and demonstrate understanding of their roles in identifying, protecting, detecting, responding and recovering from cyberattack	2	2018-05-22 13:34:05
3	Employees and third parties who have access to information systems and software demonstrate understanding of their roles and responsibilities in protecting organizations physical systems and electronic access to information	3	2018-05-22 13:34:05
4	Policies and procedures have been defined and communicated to employee and third parties use of organization's information technologies	2	2018-05-22 13:34:05
5	Periodic review of employee system activity logs to inspect use, emails, file downloads and use of portable devices	4	2018-05-22 13:34:05
6	Cyber security awareness training and brown bag workshops are conducted to educate employee about phishing, identity theft, malware and spyware on annual basis	5	2018-05-22 13:34:06
7	The mission, objectives and activities have been established and communicated to employee and third parties	2	2018-05-22 13:34:06
8	The organization has mapped how information and data moves through the organization	3	2018-05-22

[Download Scores](#)

© 2018 Copyright: For Msc. Research of Kabarak University (Edwin Limo)

Figure 25: Scores GUI
Source: Researcher (2018)

6. Recommendations component

The recommendation component retrieves information from the assessment database. The information contained in the recommendation advises the user on what to be implemented in order to increase the cyber readiness of the organization. The recommendations are reached at by filtering the recommendations for all the questions whose assessment scores are below the threshold. It further allows the user to download the recommendations in form of PDF. The Figures 26 and 27 presents the logic flowchart and GUI presentations respectively.

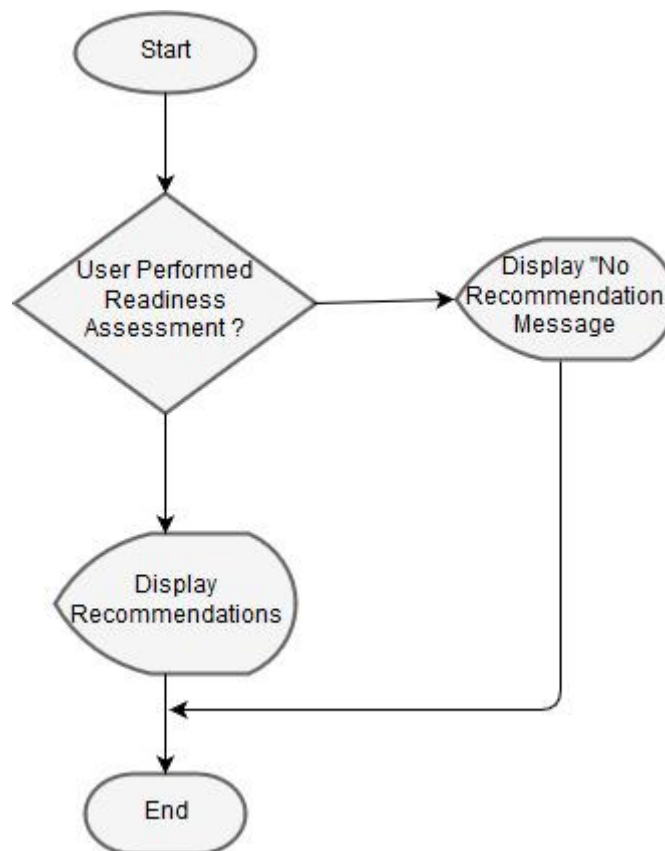


Figure 26: Recommendations Flowchart
Source: Researcher (2018)

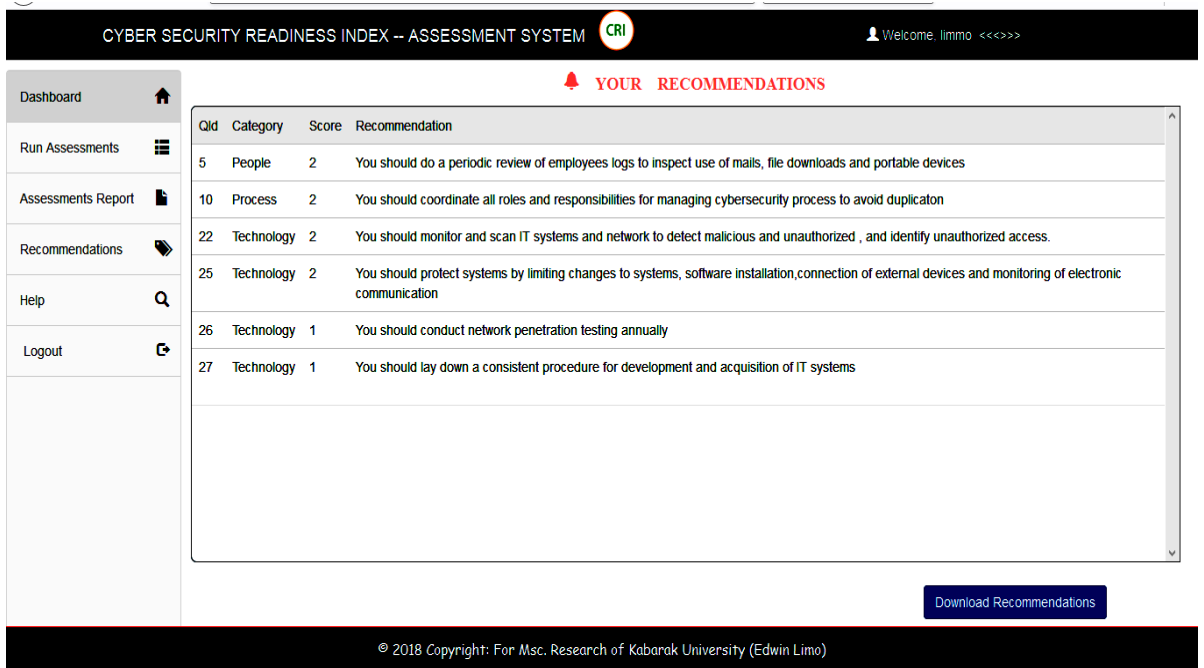


Figure 27: Recommendation GUI
Source: Researcher (2018)

7. Help Module

Help module contains information that provides the guidance on how to navigate the CRI system and perform system functions. This module is helpful to users who interact with the system for the first time. Figure 28 shows the help GUI layout.

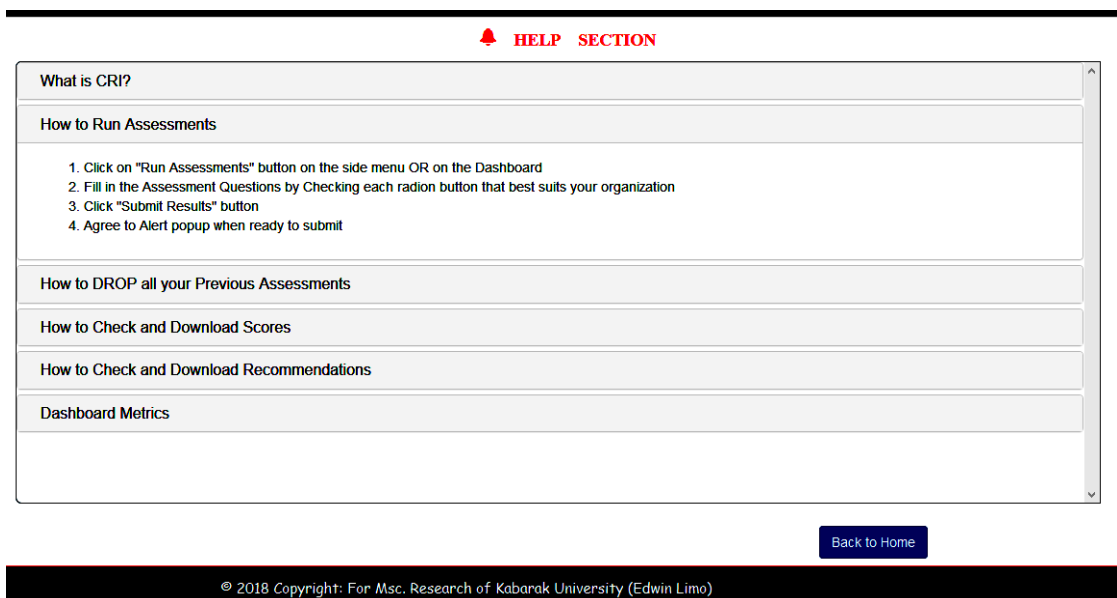


Figure 28: Help GUI
Source: Researcher (2018)

8. Home Page

This component presents a responsive home page that allows the user to make quick navigations, view graphical presentation of cyber readiness, view cyber readiness as per each cyber element. The user is also able to view the number of recommendations given and the number of assessments done. The Figure 29 shows a graphical user interface layout of home display component.

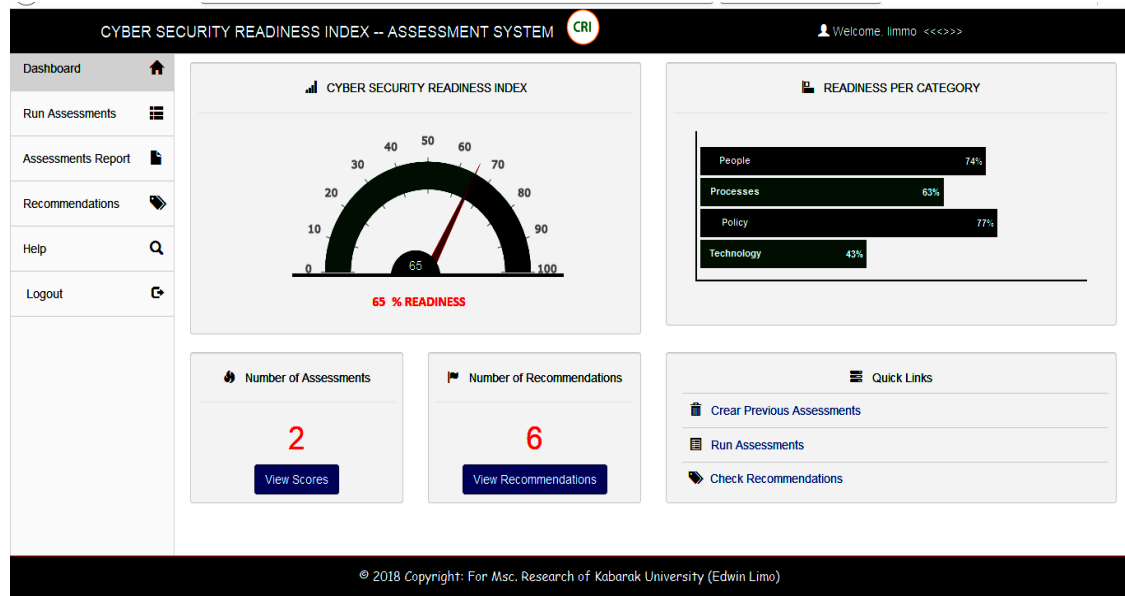


Figure 29: Home GUI
Source: Researcher (2018)

4.10.7 System evaluation

The evaluation of CRI system employed three different types of evaluation namely; IT-Systems as such Goal-based evaluation approach, cognitive walkthrough and heuristic evaluation approach. Table 11, table 12 and table 13 shows how the evaluation was done.

1. IT System as Such' Goal Based Evaluation

IT-Systems as such Goal-based evaluation approach is a type of evaluation that determines the extent at which the system is achieving the pre-set objectives (Youker, 2014). IT-systems as such evaluation does not involve the users but rather an evaluator and the IT-system involved. The outcome of the evaluation is based on how the evaluator understands the organization and how the system will support it (Cronholm, 2004). Table 4.9 shows the pre-set objectives and the final results.

Table 4.9: IT System as Such' Goal Based Evaluation

Objective	Results
1. User registration: The system was to allow users to register by entering personal details which were stored in the database.	a) The prototype was able to allow users to register by inputting: User name, organization's name, email and password. b) The prototype was able to store validated user registration details in MySQL database.
2. User login and Authentication: The prototype was to prompt users to provide user credentials in order to access the system's functionalities.	a) The prototype prompted the user to enter email and password in order to login. b) The prototype grants access to the users when the login details matches the information in the database provided during registration for authentication purposes.
3. Readiness Assessment and submission: The prototype was retrieve questions from the database and present to the user for assessment. After dully filling the questions the user was to submit.	a) The prototype was able to pull the questions from the database and present to the user in a Likert scale format. b) After filling the questions the prototype allowed the user to submit back the dully filled form.
4. CRI Computation: The prototype was expected to compute the cyber security readiness index and present it inform of a graph.	a) The prototype was able compute the CRI by reading the users score from the database b) The prototype was able to present the readiness index using both bar and speedometer gauge.
5 Scores and recommendations: The prototype was expected to retrieve scores and downloadable recommendations	a) The prototype was able to pull both scores and recommendations from the database b) The user was also able to download the recommendations in PDF form.

2. Heuristic Evaluation

Heuristic evaluation is a usability test done by an expert. Heuristic evaluation approach involves having an expert reviewing the system against set guidelines (Khajouei et al., 2016). CRI system was reviewed against Nielsen 10 heuristic principles. Table 4.10 below shows the 10 Nielsen principles and the evaluation results.

Table 4.10: Heuristic Evaluation

	Heuristic principle	Results
1.	Visibility of system status	CRI system informs the user about what is going on through appropriate feedback
2.	Match between system and the real world	The CRI uses simple phrases that is understood by the user
3.	User control and freedom	CRI system is designed in such a way that the user has the impression that they are in control of the system
4.	Consistency and standards	The system is consistent this is because the design standards and conventions were observed
5.	Error prevention	The interface is designed in such a way that it is hard to make errors
6.	Recognition rather than recall	The user can save the password so as to auto remember. It is advisable to use this on a personal computer for security reasons.
7.	Flexibility and efficiency of use	The CRI contains shortcuts the helps the first time assesses to navigate through the system
8.	Aesthetic and minimalist design	The interface contains only the necessary information and no any extraneous information
9.	Help users recognize, diagnose, and recover from errors	The System expresses errors in plain text e.g. “you have not done assessment therefore you have no recommendations”
10.	Help and documentation	The CRI system provides guidance on how to operate the system through the help module.

3. Cognitive Walkthrough Evaluation

Cognitive walkthrough approach is designed to test whether new users can easily carry out task with ease (Georgsson & Kushniruk, 2016). After the CRI system was deployed online users were asked to register and perform assessment to ascertain the ease of learning the system. Several concerns were raised and rectified immediately.

4.10.8 Validation Process

After the CRI model was complete the system was deployed online and users were allowed to register, login and perform independent cyber security readiness index assessment. Five hospitals namely; Bahati District Hospital, Nairobi women Hospital, Nakuru nursing Home, Mediheal Hospital and Valley Hospital were selected for the validation of the system after being assured of their anonymity. It was ascertained the system could capture the user's details and store them in the database. Figure 30 below shows the administrator view with the names of the users from different hospitals that performed the readiness assessment, Encrypted password (SHA-256) and their respective cyber security index.

	user_name	password	assessmentdate	▼ CRI
<input type="checkbox"/>	Amos	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92	2018-08-23 12:16:04	73.6
<input type="checkbox"/>	Limmo	fc1f09ab08ebdd072ea6da53a5691abcc18c9163b1be1f0921a5adb50e3f5077	2018-05-01 06:40:33	63.0
<input type="checkbox"/>	Joshua	641e41ef0a4a50a456597637bfefc01d2162f363105ed5570d81d28bbb59c835	2018-05-22 12:54:20	61.4
<input type="checkbox"/>	Gladys	641e41ef0a4a50a456597637bfefc01d2162f363105ed5570d81d28bbb59c835	2018-05-01 10:11:55	58.8
<input type="checkbox"/>	Festus	f57776bda99f58774d3bf66893b1ee15be87853cd87c4efe6737520d35173fb3	2018-08-23 12:19:22	50.6
<input type="checkbox"/>	Mercy	e640b1bbc1441dfa1c05a0f8f0e3c089b3f516eb7f10376fc078e4c79a3956b5	2018-08-23 12:22:55	49.8
<input type="checkbox"/>	edu	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92	2018-07-31 07:06:56	21.4

Figure 30: Model Verification and Validation
Source: Researcher (2018)

4.10.9 Model Case Scenario Evaluation

This section demonstrates the possible graphical result scenarios

1. Worst case scenario

Worst case scenario is obtained when a user scores an average score of 1 for every assessment question

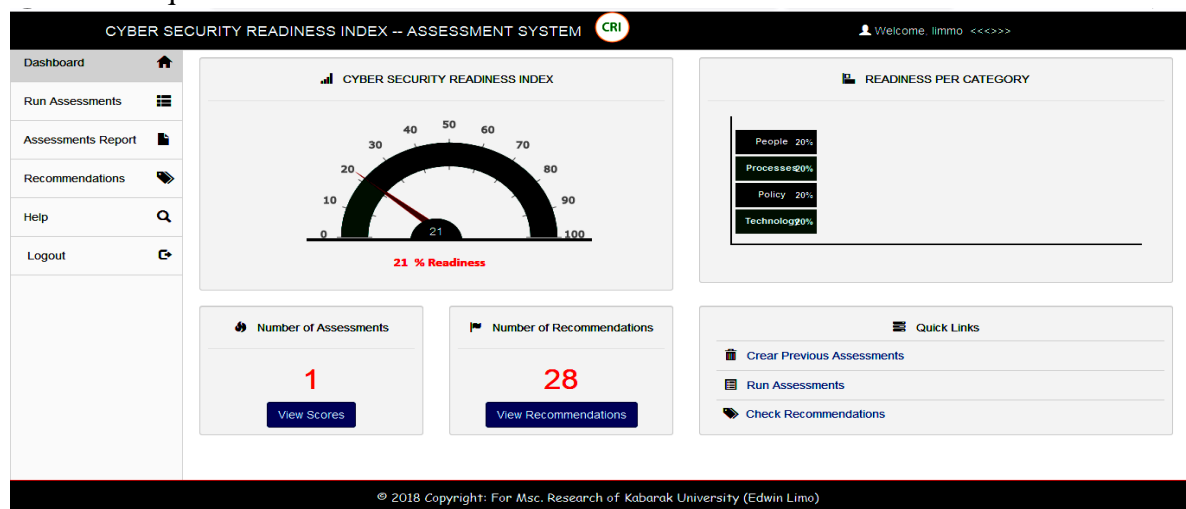


Figure 31: Worst Case Scenario GUI
Source: Researcher (2018)

2. Average case scenario

Average case scenario is reached at when a user scores an average of 2.5

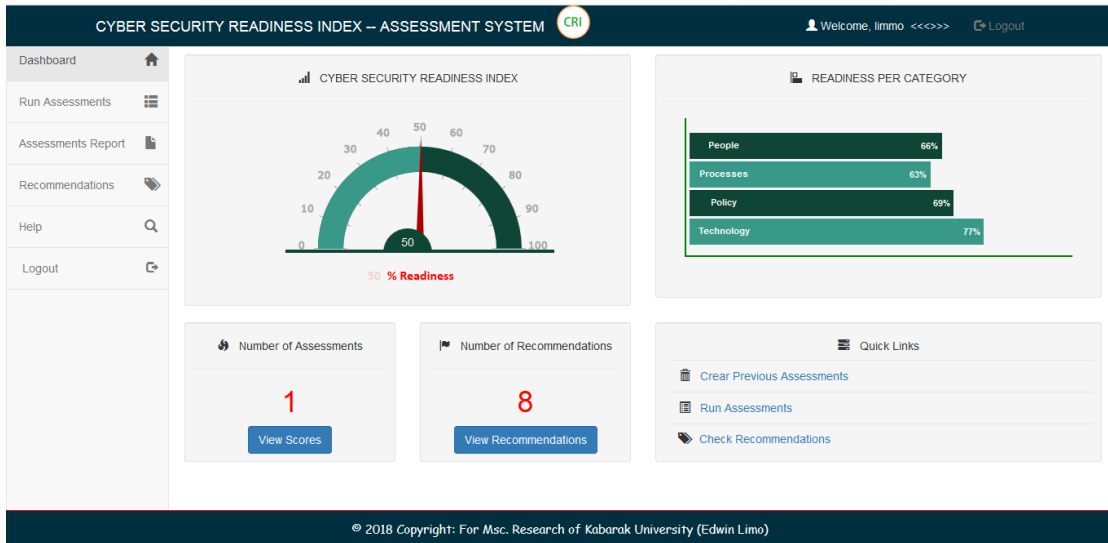


Figure 32: Average Case Scenario GUI
Source: Researcher (2018)

3. Best case scenario

Best case scenario is achieved when a user scores an average score of 5 in every assessment question.

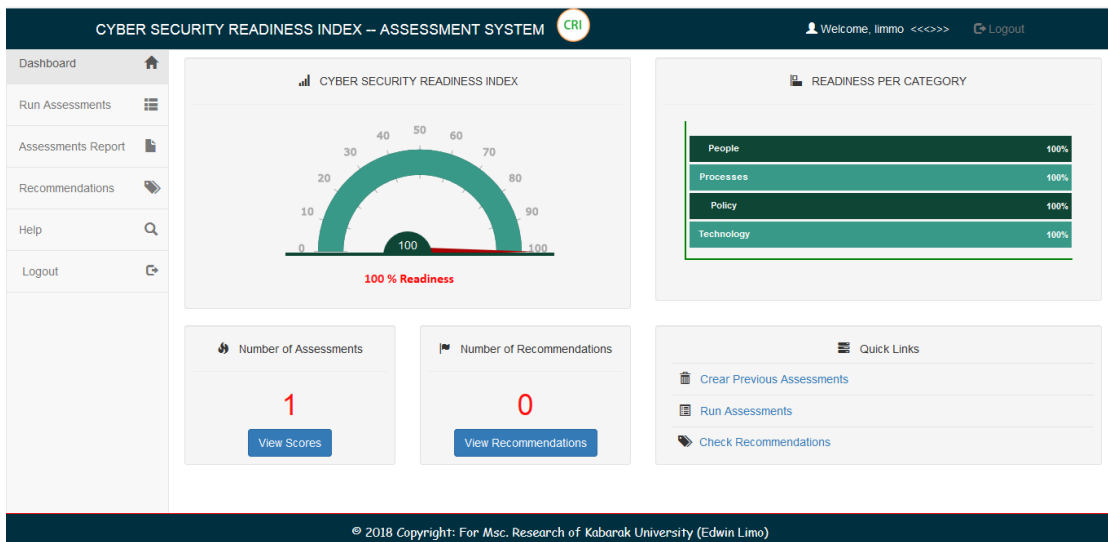


Figure 33: Best Case Scenario GUI
Source: Researcher (2018)

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents conclusion, how each objective of the research was met. It goes ahead to give conclusion on the model and finally giving the recommendations.

5.2 Summary

This study aimed at solving the problem of cybersecurity among the healthcare sector. Over the past decades healthcare industry has lagged behind in protecting its infrastructure against cyber threats. This has made the industry lucrative to attackers due to ease of attack and valuable information the industry possesses. Therefore, this study was based on the need to have healthcare industry aware of how ready they are in protecting its assets. This necessitated the development of CRI a model to assist the healthcare determine their readiness level based on the four elements affecting cyber security; people, process, technology and policy. The model was implemented as web-based application. With CRI a user is able to register, login, perform readiness assessment and download recommendations.

5.3 Conclusion

Cybercrime menace is the talking point for every organization that is operating on digital world this age. Healthcare sector is an example of institutions that has been hit hard by the menace, this is evident by the number of attacks that have been experienced lately by hospitals. Healthcare sector face increased cyber risks compared to other sectors such as financial, retail and government, this is due valuable information the healthcare hold. This information is lucrative to attackers and that is why healthcare is the prime target for attackers. Cybercrime is starting to evolve and it is evolving at a worrying pace. Few decades ago no one expected that hospitals would be ranked among the most attacked sectors. The solution lies with the healthcare sector, first they need to acknowledge the impacts of cybercrime and start investing on its infrastructure starting from the workforce to the safety of clinical devices they use.

Though no organization is 100 per cent cyber ready, healthcare sector has a long way to go in protecting its infrastructure. As long as hospitals continue to embrace digitalization then cybercrime is here with us to stay. The development of CRI was to aid the healthcare sector assess its readiness to cybercrime and also provide

recommendations on what should be implemented in order to improve its readiness. More detailed conclusions on whether the specific objectives were achieved and how is discussed below in sections 6.1.1.

5.3.1 Objectives Address

This sections discusses how each specific research objective was achieved

1. Research Question 1: How will the elements affecting cybersecurity readiness index in adoption of eHealth be assessed?

The research question 1 was achieved by checking on the criticality of the four elements affecting cybersecurity which are the people, process, policy and technology. Respondents were asked to rate the four elements of cybersecurity based on their criticality in regard to their respective hospitals. The study established that of the four cybersecurity elements, policy was rated the most critical of the four followed by technology, people and process respectively. According to Schaeffer et al. (2009) organizations must have policies in respect to data retention, privacy, data protection and data destruction. Many hospitals seems to be in agreement with Schaeffer's statement.

2. Research Question 2: How will the model for computing cybersecurity readiness index in adoption of eHealth be developed?

A mathematical model approach was employed in developing Cybersecurity Readiness Index (CRI). After doing a correlation between the cybersecurity readiness and each of the four elements affecting cyber security (people, process, technology and policy) a regression analysis was done in order to establish respective weights. A multiple regression equation was used since the predictable variables were more than two, this made it possible to factor in the four variables. The design of cybersecurity readiness system focused on the four elements affecting cyber security.

3. Research Question 3: How will the prototype of a web based application for computing cybersecurity readiness index be implemented?

CRI prototypes was designed as a web based application that can be accessed online. MySQL was used as a database engine, Bootstrap for the responsive front-end, and PHP as a server-side language. The database is made up of tables for storing assessment questions, user's information and assessment information. When a use runs an assessment, assessment questions are pulled from the database. After dully filling the questions the user submits back the filled questions. After subjecting the scores to the regression equation, the user can view the results for cybersecurity

readiness index. The cumulative results are presented in the form of a bar graph while each cybersecurity element result is presented in the form of a speedometer gauge. Finally the user can download recommendations based on his score.

4. Research Question 4: How will the model be verified and validated?

The model for computation of cyber security readiness index was deployed online by hosting it. Users were allowed to register and login into the system. After successfully logging into the system, the users were allowed to perform some tasks such as; running an assessment, viewing their readiness status, viewing assessment scores and finally downloading the recommendations. All these tasks verified the system that it performs the intended functionalities. User details were stored in the database after validation and passwords encrypted. User scores were also stored after validation and used to compute SREI and retrieve recommendations accurately.

5.3.2 Recommendations

This section presents the recommendations that this study is proposing.

(i) Adoption of CRI in other Organizations

During the course of this study it was established that almost all organizations are faced with cybersecurity threats and not only hospitals. This calls for strict measures to be put in place in order to curb the menace. Cybersecurity readiness index system can be improved such that other organizations not necessarily hospitals can perform their readiness index and be able to understand the security posture of each element of cybersecurity affecting their respective organizations.

(ii) Centralized Management

Though CRI system is a web based system meaning it can be accessed online where users can register, login and perform independent assessment, the researcher recommends the need to have a centralized management point. This unit can be a regulatory body or government body that will manage the database. This will help in regulating the system such that anonymous users may not register or give falsified information. This will also help in protecting sensitive data provided by the hospitals

(iii) Imposed Compliance

The ministry of Health need to incorporate this model to their oversight role of the healthcare sector. Ministry of health can give a policy that all hospitals should be able to check their cyber readiness online in order to guarantee patients safety. This will

give the hospital a clear snapshot of the effectiveness of its existing cyber measures and the preparedness in handling cyber risks and in turn help in detecting, preventing, containing, and responding to changing cyber threats.

5.3.3 Recommendation for further research.

During the course of this research study, areas of further study were established. Further research should be done on the cyber readiness of the medical devices. It was noted that most hospitals still use outdated medical devices, this provides an easy way for hackers to attack. Even if the healthcare sector are able to manage the cybersecurity elements (people, process, policy, and technology) and still use outdated medical devices then their effort is worth nothing

REFERENCES

- Ahlstrom, J., & Zoline, K. (2018). Healthcare Security Readiness and Maturity Assessment. In *Healthcare Security Readiness and Maturity Assessment* (p. pg 8). Las Vegas. Retrieved from <https://healthitsecurity.com/news/78-of-healthcare-workers-lack-data-privacy-security-preparedness>
- Alfaro, R. (2016, November 17). Vertical privilege escalation. Retrieved October 19, 2017, from <https://outpost24.com/vertical-privilege-escalation>
- Akouwah, F., Yuan, X., Xu, J., & Wang, H. (2012, January). An overview of laws and standards for health information security and privacy. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- Andrews, M. (2016, August 25). The Rise of Medical Identity Theft. Retrieved September 25, 2017, from <https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/>
- Ashoor, A. S., & Gore, S. (2011, July). Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). In *International Conference on Network Security and Applications* (pp. 497-501). Springer, Berlin, Heidelberg.
- Ashenden, D. (2008). Information security management: A human challenge?. Information security technical report, 13(4), 195-201. Ashenden, D. (2008). Information security management: A human challenge?. *Information security technical report*, 13(4), 195-201.
- Bayuk, J., & Price Waterhouse, L. L. P. (1997). Security through process management. *Price Waterhouse*.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548
- Budryk, Z. (2015, April 29). 4 essential steps for healthcare compliance | FierceHealthcare. Retrieved from <https://www.fiercehealthcare.com/healthcare/4-essential-steps-for-healthcare-compliance>
- Bloomberg, B., Cooper, D. R., & Schindler, P. S. (2011). Business research methods.
- Brahima, S. (2017). Global Cybersecurity Index 2017. *International Telecommunication Union (ITU)*, 1-77.
- Calder, A., & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd..
- Cisco Press. (2016, January 25). Retrieved October 02, 2017, from <http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3>

- Cotenescu, V. M. (2015). People, Process, And Technology; A Blend To Increase An Organization Security Posture.
- Convery, S. (2009, February 14). Network Authentication, Authorization, and Accounting: Part One - The Internet Protocol Journal - Volume 10, No. 1. Retrieved October 18, 2017, from <http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html>
- Cowie, M. R., Bax, J., Bruining, N., Cleland, J. G., Koehler, F., Malik, M., ... & Vardas, P. (2016). e-Health: a position statement of the European Society of Cardiology. *Eur Heart J*, 37(1), 63-66.
- Culp, S. (2016, May 10). Cyber Risk: People Are Often The Weakest Link In The Security Chain. Retrieved September 15, 2017, from <https://www.forbes.com/sites/steveculp/2016/05/10/cyber-risk-people-are-often-the-weakest-link-in-the-security-chain/#e1f111a2167a>
- Chakraborty, N. (2013). Intrusion detection system and intrusion prevention system: A comparative study. *International Journal of Computing and Business Research (IJCBR) ISSN (Online)*, 2229-6166.
- Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). Cyber Readiness Index 2.0.
- Durbin, S. (2016, May 24). Insiders are today's biggest security threat. Retrieved September 18, 2017, from <https://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin>
- Drevin, L., Kruger, H., Bell, A. M., & Steyn, T. (2017, May). A Linguistic Approach to Information Security Awareness Education in a Healthcare Environment. In *IFIP World Conference on Information Security Education* (pp. 87-97). Springer, Cham.
- Farlex, I. N. C. (2009). The free dictionary. Retrieved June, 28, 2012.
- Ferran, T. (2014, May 9). What Are Addressable HIPAA Requirements? Retrieved October 10, 2017, from <http://blog.securitymetrics.com/2014/05/addressable-hipaa-requirements.html>
- Freeborn, A. (2017, August 28). ISO/IEC27000: Removable Media. Retrieved November 03, 2017, from <https://www.tenable.com/sc-dashboards/isoiec27000-removable-media>
- Gardner, J. (2009). Authentication and Authorization. *The Definitive Guide to Pylons*, 415-432.
- Gambo, I. P., & Soriyan, A. H. (2017). ICT Implementation in the Nigerian Healthcare System. *IT Professional*, 19(2), 12-15.

- Georgsson, M., & Kushniruk, A. (2016, June). Mediating the Cognitive Walkthrough with Patient Groups to achieve Personalized Health in Chronic Disease Self-Management System Evaluation. In *pHealth* (pp. 146-151).
- Golchha, P., Deshmukh, R., & Lunia, P. (2015). A Review on Network Security Threats and Solutions. *International Journal of Scientific Engineering and Research*, 3(4), 21-24.
- György, S. (2012, August). CMM capability maturity model.
- Hao, S., Syed, N. A., Feamster, N., Gray, A. G., & Krasser, S. (2009, August). Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine. In *USENIX security symposium* (Vol. 9).
- Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: Is the US healthcare system safe?. *Telemedicine and e-Health*, 19(1), 61-66.
- Institute, InfoSec, and InfoSec Resources. "Why Security Awareness Training In Healthcare Must Be Part Of Your Security Strategy." InfoSec Resources. N.p., 2016. Web. 22 Sept. 2017.
- ISO/IEC, (2005). ISO/IEC 27001:2005 *Information Technology. Security Techniques. Specification for an Information Security Management System*. Geneva, Switzerland: ISO/IEC.
- Janes, P. (2013). People, process, and technologies impact on information data loss.
- Janes, P. 2012. People, Process, and Technologies Impact on Information Data Loss. Accessed 7 December 2014. <http://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impactinformation-data-loss-34032>
- Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., ... & Shitanda, S. (2015). *Kenya Cyber Security Report 2015*. Serianu Limited.
- Killian, T. J., Altom, M. W., Garay, J. A., Nortz, D., & Segelstein, D. J. (2014). U.S. Patent No. 8,762,707. Washington, DC: U.S. Patent and Trademark Office.
- Kokko, K. (2017). Next-generation firewall case study.
- Kosutic, D. (2016, May 30). ISO 27001 Information Security Policy? What should you include? Retrieved from <https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/>
- Kumar, A., & Singh, H. (2014). Network Security: A Literature Review.
- Kuhlthau, C. C. (2004). *Seeking meaning: A process approach to library and information services*. Libraries Unltd Incorporated.
- Khajouei, R., Zahiri Esfahani, M., & Jahani, Y. (2017). Comparison of heuristic and cognitive walkthrough usability evaluation methods for evaluating health

- information systems. *Journal of the American Medical Informatics Association*, 24(e1), e55-e60.
- Khoumsi, A., Erradi, M., & Krombi, W. (2016). A formal basis for the design and analysis of firewall security policies. *Journal of King Saud University-Computer and Information Sciences*.
- Lee, J., Lee, D., & Kang, S. (2007). An overview of the business process maturity model (BPMM). *Advances in web and network technologies, and information management*, 384-395.
- Leibovitz, M. (2013, February 28). Wireless Networking in Healthcare: A Global Healthcare Study. Retrieved from <http://www.extremenetworks.com/the-state-of-wireless-networking-in-healthcare-a-global-healthcare-study/>
- Lu, R., Sadiq, S., & Governatori, G. (2007, September). Compliance aware business process design. In *International Conference on Business Process Management* (pp. 120-131). Springer, Berlin, Heidelberg.
- Luo, Y., & Bu, J. (2016). How valuable is information and communication technology? A study of emerging economy enterprises. *Journal of World Business*, 51(2), 200-211.
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?.
- Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity Challenges and Compliance Issues within the US Healthcare Sector. *International Journal of Business and Social Research*, 5(2), 55-66.
- McKay, V. (2016). *What is the Capability Maturity Model? (CMM) | Process Maturity FAQ*. [online] Selectbs.com. Available at: <http://www.selectbs.com/process-maturity/what-is-the-capability-maturity-model> [Accessed 11 Oct. 2017].
- Mugenda, A. (2003). Research methods Quantitative and qualitative approaches by Mugenda. *Nairobi, Kenya*.
- Ngechu, C. R. (2004). Research methodology: Methods and techniques.
- Oberheide, J., Cooke, E., & Jahanian, F. (2008, July). CloudAV: N-Version Antivirus in the Network Cloud. In *USENIX Security Symposium* (pp. 91-106).
- Olavsrud, T. (2012, August 15). How to Secure Data by Addressing the Human Element. Retrieved from http://www.cio.com/article/713753/How_to_Secure_Data_by_Addressing_the_Human_Element
- Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE software*, 10(4), 18-27.

- Patil, S., Rane, P., & Meshram, D. B. (2012). Ids vs ips. Proceedings of *International Journal of Computer Networks and Wireless Communications*, 2.
- Paganini, P. (2012). Why humans could be the weakest link in cyber security chain. Retrieved August, 21, 2015.
- Patten, M. L. (2007). Understanding research methods . Glendale. CA: *Pyrzczak Publishing*. Pinto, G., Bigozzi, L., Gamannossi, B., & Vezzany, C.(2012). Emergent literacy and early writing skills. *The Journal of Genetic Psychology*, 173(3), 330-354.
- Perakslis, E. D. (2014). Cybersecurity in health care. *N Engl J Med*, 371(5), 395-397.
- People. (n.d.).In *Merriam-webster dictionary*. Retrieved from <https://www.merriam-webster.com/dictionary/people>
- Policy.(n.d.). In wikipedia. Retrieved from <https://en.wikipedia.org/wiki/Policy>
- Ponemon Institute LLC. (2012, July). 2012 Confidential documents at risk study (PonemonInstitute Research Report). Retrieved from http://www.ciosummits.com/media/pdf/solution_spotlight/Ponemon%20White%20Paper%20FINAL.pdf
- Qian, Z., Mao, Z. M., Xie, Y., & Yu, F. (2010, March). On Network-level Clusters for Spam Detection. In *NDSS*.
- Rajab, M. A., Ballard, L., Lutz, N., Mavrommatis, P., & Provos, N. (2013, February). CAMP: Content-Agnostic Malware Protection. In *NDSS*.
- Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2006). Research methodology. *arXiv preprint physics/0601009*.
- Rohloff, M. (2009). Process management maturity assessment. *AMCIS 2009 Proceedings*, 631.
- Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling control objectives for business process compliance. *Business process management*, 149-164.
- Sabale, R. G., & Dani, A. R. (2012). Comparative study of prototype model for software engineering with system development life cycle. *IOSR Journal of Engineering*, 2(7), 21-24.
- Schaeffer, B. S., Chan, H., Chan, H., & Ogulnick, S. (2009). *Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others*.
- Spence, N., Paul III, D. P., & Coustasse, A. (2017). *Ransomware in Healthcare Facilities: The Future is Now*.
- Wong, C., Odom, S. L., Hume, K. A., Cox, A. W., Fettig, A., Kucharczyk, S., ... & Schultz, T. R. (2015). Evidence-based practices for children, youth, and young adults with autism spectrum disorder: A comprehensive review. *Journal of Autism and Developmental Disorders*, 45(7), 1951-1966.

- What is Process Awareness . (2014, February 12). Retrieved October 02, 2017, from <http://www.taskmanagementguide.com/glossary/what-is-process-awareness-.php>
- Vesely, R. (2017, June 06). Report: Health care cybersecurity unprepared and under threat. Retrieved November 10, 2017, from <https://healthjournalism.org/blog/2017/06/report-health-care-cybersecurity-unprepared-and-under-threat/>
- What is a Web-Based Application? - Definition from Techopedia.* (2018). *Techopedia.com*. Retrieved 24 January 2018, from <https://www.techopedia.com/definition/26002/web-based-application>
- Wiech, D. (2015). *How to Improve Access Security in Healthcare*. [online] Infosecurity Magazine. Available at: <http://www.infosecurity-magazine.com/opinions/improve-access-security-in/> [Accessed 9 Oct. 2017].
- Williams, View. "New Healthcare Report Shows Importance Of A Security Awareness Program." Samsung Business Insights. N.p., 2016. Web. 17 Sept. 2017.
- Wim, A. (2015). KPMG Survey of Corporate Responsibility Reporting 2015. Retrieved from <https://home.kpmg.com/xx/en/home/insights/2015/11/kpmg-international-survey-of-corporate-responsibility-reporting-2015.html>
- Wharton, C., Rieman, J., Lewis, C., & Polson, P. (1994, June). The cognitive walkthrough method: A practitioner's guide. In *Usability inspection methods* (pp. 105-140). John Wiley & Sons, Inc..
- Youker, B. W. (2014). Goal-free Evaluation and Goal-Based Evaluation
- Zamora, W. (2016, March 28). How to create a successful cybersecurity policy. Retrieved September 20, 2017, from <https://blog.malwarebytes.com/101/2016/03/how-to-create-a-successful-cybersecurity-policy/>
- 10 Steps to Cyber Security. (2016, August 04). Retrieved October 16, 2017, from <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

Appendix I: Hospitals selected for the Research

No.	Name of the Hospital	Category
1	Nakuru County Referral Hospital	Public
2	Bahati District Hospital	Public
3	Molo District Hospital	Public
4	Mediheal	Private
5	Evans Hospital	Private
6	Valley Hospital	Private
7	Nairobi Women Hospital	Private
8	Karen Hospital	Private
9	Aga Khan Hospital	Private
10	Egerton University Hospital	private
11	Nakuru Nursing Home	Private

Appendix II: Questionnaire

I am a Master of Science Information Technology (IT) student of Kabarak University conducting a research on “A web-based model to determine cyber security readiness index for hospitals in Kenya. “This is request you to answer the questions outlined below to the best of your knowledge. Note that the information provided will only be used for academic purpose and will be protected by strict ethical standards of anonymity.

PART A: GENERAL QUESTIONS

Please tick the most appropriate answer in this section

1. What category does your Hospital fall into?

- (i) Public Hospital [] (ii) Private Hospital []

2. What position do you hold in the Hospital?

- (i) System administrator [] (ii) Medical records manager []
(iii) HR manager [] (iv) Database administrator []
(v) ICT manager []

PART B: SPECIFIC QUESTIONS

- 3.** In a scale of 1 to 5, to what extend do you think the following cybersecurity elements affect your hospital (**KEYS: 1=Not Very Critical, 2=Not Critical, 3=Neutral, 4=Critical, 5=Very Critical**)

NO	Question	1	2	3	4	5
1	People					
2	Process					
3	Policy					
4	Technology					

PART C: QUESTIONS

In the scale of 1 to 5, please tick the most appropriate answer to the questions in relation to cybersecurity elements; people, process, policy and technology (**KEYS:** *1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree*)

4. PEOPLE

NO.	Questions	1	2	3	4	5
1	Cybersecurity responsibilities and roles have been identified and communicated to employees including third parties					
2	All senior management, employees and third parties have received training and demonstrate understanding of their roles in identifying, protecting, detecting, responding and recovering from cyberattack					
3	Employees and third parties to have access to information systems and software demonstrate understanding of their roles and responsibilities in protecting organizations physical systems and electronic access to information					
4	Policies and procedures have been defined and communicated to employee and third parties use of organization's information technologies					
5	Periodic review of employee system activity logs to inspect use, emails, file downloads and use of portable devices					
6	Cyber security awareness training and brown bag workshops are conducted to educate employee about phishing, identity theft, malware and spyware on annual basis					
7	The mission, objectives and activities have been established and communicated to employee and third parties					

5. PROCESS

NO.	Questions	1	2	3	4	5
1	The organization has mapped how information and data moves through the organization					
2	The organization has identified and documented known cybersecurity threats and the potential impact of unauthorized access to information and used this information to determine organization's level					
3	All roles and responsibilities for managing cybersecurity processes are coordinated to avoid duplication and are aligned to the employees position					
4	The organization has identified and prioritized all activities essential for its' operation					
5	All cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat					
6	All cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat					
7	The environment outside of IT systems is monitored for unauthorized access					

6. POLICY

NO	Questions	1	2	3	4	5
1	Access to areas outside of the IT system is restricted, especially in areas where computers, devices, and files that contain sensitive information are kept					
2	IT systems and data removal, transfer, storage, and destruction is standard throughout the organization					
3	Permissions for users, devices, and software access to organization IT systems, equipment, and files is limited to only what is necessary to perform job functions or ensure normal functioning					
4	Personnel understand the legal and regulatory requirements governing cybersecurity					
5	Remote access is managed through formal approval and credentialing based on the role of the employee or third-party					
6	Cybersecurity policies are continuously tested to determine their usefulness against new and emerging threats and how well they comply with industry best practices, which are continuously improved through incorporation of lessons learned					
7	All users and devices undergo a standard approval process prior to use and their system identities and credentials are managed by designated authorized personnel					

7. TECHNOLOGY

NO.	Questions	1	2	3	4	5
1	The IT systems, the network, software, and third party activity is monitored and scanned to detect malicious and unauthorized code, and identify unauthorized access					
2	All information and data that is stored, transmitted, or accessed by the organization is protected from unauthorized access					
3	All IT systems, software, and data is scanned to identify who sent it and/or where it came from, and assess how likely the source is to be reputable					
4	IT systems are protected by limiting changes to the system, software installation, connection of external devices, monitoring electronic communications, and users of the system					
5	Network penetration testing is conducted on an annual basis					
6	Consistent procedures for development and acquisition of IT systems and software are used					
7	Software patches and updates are done on daily fashion					

PART D: QUESTIONS

In a scale of 1 to 5, to what extend do you gauge your cybersecurity Readiness for each cybersecurity elements listed below (**KEYS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree**)

8. CYBERSECURITY READINESS

NO	Question	1	2	3	4	5
1	Our cybersecurity Readiness regarding People is satisfactory					
2	Our cybersecurity Readiness regarding Process is adequate					
3	Our cybersecurity Readiness regarding Policy is sufficient					
4	Our cybersecurity Readiness regarding Technology is satisfactory					

Appendix III: NACOSTI Research Authorization



NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone: 020 400 7000,
0713 788787, 0735404245
Fax: +254-20-318245, 318249
Email: dg@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref. No. **NACOSTI/P/18/52722/21744**

Date: **16th March, 2018**

Aiyabei Kiplimo Edwin
Kabarak University
P.O. Private Bag 20157
KABARAK.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on "*A web-based model to determine cyber security readiness index for hospitals towards adoption of e-health*" I am pleased to inform you that you have been authorized to undertake research in **Nakuru County** for the period ending **15th March, 2019**.

You are advised to report to **the County Commissioner and the County Director of Education, Nakuru County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit a **copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

DR. STEPHEN K. KIBIRU, PhD.
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The County Commissioner
Nakuru County.

The County Director of Education
Nakuru County.

Appendix IV: Ministry of Education Research Authorization

**MINISTRY OF EDUCATION
STATE DEPARTMENT OF BASIC EDUCATION**

Telegrams: "EDUCATION",
Telephone: 051-2216917
When replying please quote



COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY
P. O. BOX 259,
NAKURU.

Ref.CDE/NKU/GEN/4/21/VOL.VI/27

21st March, 2018

TO WHOM IT MAY CONCERN

RE: RESEARCH AUTHORIZATION -AYABEI KIPLIMO EDWIN
NACOSTI/P/18/52722/21744

Reference is made to **NACOSTI/P/18/52722/21744 dated 16th March, 2018**

Authority is hereby granted to the above named to carry out research on "**A web-based model to determine cyber security readiness index for hospitals towards adoption of e-health in Nakuru County**" for a period ending **15th March, 2019.**

Kindly accord him the necessary assistance.

A handwritten signature in black ink, appearing to read 'Akoko Okayo'.

AKOKO OKAYO
FOR: COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY

Copy to:-

- Kabarak University
P.O Private Bag 20157
KABARAK

**Appendix V: Ministry of Interior and Co-ordination on National Government
Research Authorization**



**THE PRESIDENCY
MINISTRY OF INTERIOR AND
CO-ORDINATION OF NATIONAL GOVERNMENT**

Telegram: "DISTRICTER" Nakuru
Telephone: Nakuru 051-2212515

DEPUTY COUNTY COMMISSIONER
NAKURU EAST SUB COUNTY
P.O. Box 81
NAKURU.

Ref No. EDU 12/10 VOL. V/218

21st March, 2018

TO WHOM IT MAY CONCERN

RE:- AIYABEI KIPLIMO EDWIN

The above named has been authorized to carry out research on "**a web-based model to determine cyber security readiness; index for hospitals toward; adoption of e-health**" in Nakuru East Sub County for a period ending 15th March, 2019.

Please accord him all the necessary support to facilitate the success of his research.


**EDITH KOECH
FOR DEPUTY COUNTY COMMISSIONER
NAKURU EAST SUB COUNTY**

Appendix VI: NACOSTI Research Clearance Permit



THIS IS TO CERTIFY THAT:
MR. AIYABEI KIPLIMO EDWIN
of KABARAK UNIVERSITY, 291-30700
ELDORET, has been permitted to conduct
research in Nakuru County

on the topic: A WEB-BASED MODEL TO
DETERMINE CYBER SECURITY
READINESS INDEX FOR HOSPITALS
TOWARDS ADOPTION OF E-HEALTH

for the period ending:
15th March, 2019



Applicant's
Signature


Permit No : NACOSTI/P/18/52722/21744
Date Of Issue : 16th March, 2018
Fee Received :Ksh 1000



Director General
National Commission for Science,
Technology & Innovation

CONDITIONS

1. The License is valid for the proposed research, research site specified period.
2. Both the Licence and any rights thereunder are non-transferable.
3. Upon request of the Commission, the Licensee shall submit a progress report.
4. The Licensee shall report to the County Director of Education and County Governor in the area of research before commencement of the research.
5. Excavation, filming and collection of specimens are subject to further permissions from relevant Government agencies.
6. This Licence does not give authority to transfer research materials.
7. The Licensee shall submit two (2) hard copies and upload a soft copy of their final report.
8. The Commission reserves the right to modify the conditions of this Licence including its cancellation without prior notice.


REPUBLIC OF KENYA


National Commission for Science,
Technology and Innovation

RESEARCH CLEARANCE
PERMIT

Serial No.A 17943

CONDITIONS: see back page

Appendix VII: Publication

**Mara Research Journal of Computer Science
& Information Security Vol. 3, No. 1, August
2018, Pages 23 – 33, ISSN 2518-8453**

Assessing the Cyber Security Readiness for Hospitals towards Adoption of e-Health using a Web Based Model to Compute Cyber Security Readiness Index

Aiyabei Kiplimo Edwin
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: aiyabeiedwin@gmail.com

Received: July 30, 2018

Published: August 13, 2018

Abstract

The main goal of healthcare sector worldwide is to provide quality and efficient healthcare services to citizens. With the digitalization of healthcare information and adoption of eHealth among hospitals, healthcare sector must be protected from cyber-attacks even as the threat landscape continue to escalate. Hospitals are have fallen victims to cyber breaches due to sensitive patient's data they possess. This research attempts to offer solution through design of a web-based model that will compute cyber security readiness index (CRI) for Hospitals based on the four pillars of cybersecurity; people, process, policy and technology. The model adopts the design research approach

Keywords: eHealth, cyber-attacks, model, people, process, technology, policy

© 2016 by the author(s); Mara Research Journals (Nairobi, Kenya)

Appendix VIII: System Code

*****User Registration*****

```
<?php
ob_start();
session_start();
if( isset($_SESSION['user'])!="") {
    header("Location: home.php");
}
include_once 'dbconnect.php';
$error = false;
if ( isset($_POST['btn-signup']) ) {
    // clean user inputs to prevent sql injections
    $name = trim($_POST['name']);
    $name = strip_tags($name);
    $name = htmlspecialchars($name);
    $email = trim($_POST['email']);
    $email = strip_tags($email);
    $email = htmlspecialchars($email);
    $organization = trim($_POST['Organization']);
    $organization = strip_tags($organization);
    $organization = htmlspecialchars($organization);
    $pass = trim($_POST['pass']);
```

```

        $passError = "Password must have atleast 6 characters.";
    }

    // password encrypt using SHA256();
    $password = hash('sha256', $pass);
    // if there's no error, continue to signup
    if( !$error ) {
        $query = "INSERT INTO users(userName,Organization,userEmail,userPass)
VALUES('$name','$organization','$email','$password)";
        $res = mysql_query($query);

        if ($res) {
            $errTyp = "success";
            $errMSG = "Successfully registered, you may login now";
//basic email validation
if ( !filter_var($email,FILTER_VALIDATE_EMAIL) ) {
            $error = true;
            $emailError = "Please enter valid email address.";
        } else {
            // check email exist or not
            $query = "SELECT userEmail FROM users WHERE userEmail='$email'";
            $result = mysql_query($query);
            $count = mysql_num_rows($result);
            if($count!=0){
                $error = true;
                $emailError = "Provided Email is already in use.";
            }
        }
    }
    // password validation
    if (empty($pass)){
        $error = true;
        $passError = "Please enter password.";
    } else if(strlen($pass) < 6) {
        $error = true;
    }

```

```

        $passError = "Password must have atleast 6 characters.";
    }
    // password encrypt using SHA256();
    $password = hash('sha256', $pass);
    // if there's no error, continue to signup
    if( !$error ) {
        $query = "INSERT INTO users(userName,Organization,userEmail,userPass)
VALUES('$name','$sorganization','$semail','$spassword')";
        $res = mysql_query($query);
        if ($res) {
            $errTyp = "success";
            $errMSG = "Successfully registered, you may login now";
            unset($name);

            unset($pass);
        } else {
            $errTyp = "danger";
            $errMSG = "Something went wrong, try again later...";
        }
    }
}
?>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>CRI System</title>
<link rel="stylesheet" href="assets/css/bootstrap.min.css" type="text/css" />
<link rel="stylesheet" href="style.css" type="text/css" />
</head>
<body style="background-image:url('/assets/images/bg.jpg');">
<div class="container">
    <div id="login-form">
        <form method="post" action="<?php echo htmlspecialchars($_SERVER[PHP_SELF]); ?>"
        autocomplete="off">

```

*****User Login*****

```
<?php
    ob_start();
    session_start();
    require_once 'dbconnect.php';
    // it will never let you open index(login) page if session is set
    if ( isset($_SESSION['user'])!="") {
        header("Location: home.php");
        exit;
    }
    $error = false;
    if( isset($_POST['btn-login']) ) {
        // prevent sql injections/ clear user invalid inputs
        $email = trim($_POST['email']);
        $email = strip_tags($email);
        $email = htmlspecialchars($email);
        $pass = trim($_POST['pass']);
        $pass = strip_tags($pass);
        $pass = htmlspecialchars($pass);
        // prevent sql injections / clear user invalid inputs
        if(empty($email)){
            $error = true;
            $emailError = "Please enter your email address.";
        } else if ( !filter_var($email,FILTER_VALIDATE_EMAIL) ) {

            $error = true;
            $emailError = "Please enter valid email address.";
        }
        if(empty($pass)){
            $error = true;
            $passError = "Please enter your password.";
        }
        // if there's no error, continue to login
        if (!$error) {
            $password = hash('sha256', $pass); // password hashing using SHA256
```

```

        <div id="login-form">
            <form method="post" action="<?php echo htmlspecialchars($_SERVER['PHP_SELF']); ?>"
            autocomplete="off">
                <div class="col-md-12" style="box-shadow: 1px 1px 5px 6px #888888;
                background:#FEFCF5">
                    <div class="form-group">
                        <h2 class="" style="color:#5CB85C">Login to CRI</h2>
                    </div>
                    <div class="form-group">
                        <hr />
                    </div>

                    $res=mysql_query("SELECT userId, userName, userPass FROM users
WHERE userEmail='$email'");
                    $row=mysql_fetch_array($res);
                    $count = mysql_num_rows($res); // if uname/pass correct it returns must be 1
row
                    if( $count == 1 && $row['userPass']==$password ) {
                        $_SESSION['user'] = $row['userId'];
                        header("Location: home.php");
                    } else {
                        $errMSG = "Incorrect Credentials, Try again...";
                    }
                }
            ?>
        </DOCTYPE html>
        <html>
        <head>
            <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
            <title>CRI SYSTEM</title>
            <link rel="stylesheet" href="assets/css/bootstrap.min.css" type="text/css" />
            <link rel="stylesheet" href="style.css" type="text/css" />
        </head>
        <body style="background-image:url('./assets/images/bg.jpg');">
        <div class="container">

```

```

<?php
    if ( isset($errMSG) ) {
        ?>
        <div class="form-group">
            <div class="alert alert-danger">
                <span class="glyphicon glyphicon-info-sign"></span> <?php echo
$errMSG; ?>
            </div>
        </div>
        <?php
            }
        ?>
        <div class="form-group">
            <div class="input-group">
                <span class="input-group-addon"><span class="glyphicon glyphicon-
envelope"></span></span>
                <input type="email" name="email" class="form-control" placeholder="Your Email"
value="<?php echo $email; ?>" maxlength="40" />
                </div>
                <span class="text-danger"><?php echo $emailError; ?></span>
            </div>
            <div class="form-group">
                <div class="input-group">
                    <span class="input-group-addon"><span class="glyphicon glyphicon-
lock"></span></span>
                    <input type="password" name="pass" class="form-control" placeholder="Your Password"
maxlength="15" />
                    </div>
                    <span class="text-danger"><?php echo $passError; ?></span>
                </div>
            <div class="form-group">
                <hr />
            </div>
            <div class="form-group">
                <button type="submit" class="btn btn-block btn-success pull-left" name="btn-login"
style="width: 40%;">Login</button>

```


*****User Assessment*****

INSTRUCTIONS:--

Please Fill in the Assessment Questions by Checking each radion button that best suits your organization.</div>

<div style="background:menu; color:brown;font-family:cursive;text-align:center; border-bottom:2px solid green">

(KEY: 1=Strongly Disagree, 2=Disagree,3=Neutral, 4=Agree, 5=Strongly Agree)

<p></p>

</div>

<div style="position:absolute; height:80%;overflow: auto; margin-left:15%;margin-right:0.4%;">

<form action="" method="post" >

<?php

ob_start();

session_start();

require_once 'dbconnect.php';

if(!isset(\$_SESSION['user'])) {

header("Location: index.php");

exit;

}

\$res=mysql_query("SELECT * FROM users WHERE userId=".\$_SESSION['user']);

\$userRow=mysql_fetch_array(\$res);

?>

<!DOCTYPE html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>

<title>CRI</title>

<link rel="stylesheet" href="assets/css/bootstrap.min.css" type="text/css"/>

<link rel="stylesheet" href="assets/css/index.css" type="text/css"/>

<link rel="stylesheet" href="assets/css/cri.css" type="text/css"/>

</head>

<body style="background:#EDFFDA;background:#DCEECA; overflow: hidden;">

<div><?php include('header.php');?></div>

<div><?php include('sidemenu.php');?></div><p></p></hr>

<div style="color:#002F3F; text-align:center;font-size:14px;font-weight:normal; font-family:cursive; background:menu;padding:5px;">

```

<?php
    $sql = "SELECT category,id,question FROM forensicquestions.";
    $result = mysqli_query($conn,$sql);
    $json = array();
    if (mysqli_num_rows($result) > 0) {
        echo "<table class='table table-bordered table table-hover table-sm'
style='background: #F8F8F8;'>
            <tr style='color:#002F3F;'>
                <th>NO</th>
                <th>Category</th>
                <th>Questions</th>
                <th>1</th>
                <th>2</th>
                <th>3</th>
                <th>4</th>
                <th>5</th>
            </tr>";
        while($row = mysqli_fetch_assoc($result)) {
            $stest_data[]=$row;
            $json['responses']=$stest_data;
            $radioname = $row['questionid'];
            echo "<tr>";
            echo "<td id='radiobutton'>" . $row['questionid'] . "</td>";
            echo "<td>" . $row['category'] . "</td>";

            echo "<td id='radiobutton'>" . $row['questionid'] . "</td>";
            echo "<td>" . $row['category'] . "</td>";
            echo "<td>" . $row['question'] . "</td>";
            for($i=1;$i<=5;$i++){
                echo "<td id='radiobuttons'><input type='radio'
name='$radioname' value='$i'></td>";
            }

            echo "</tr>";
        }
        echo "</table>";
    }else {
        echo "<p id='complete'>No Questions in the database!</p>";
    }
}

```

```

        echo json_encode($json);
    }
    if(isset($_POST["submit_questionnair_btn"])){
        $sql = "SELECT questionid, question FROM assessmentquestions";
        $result = mysql_query($sql);
        while($row = mysql_fetch_assoc($result)) {
            $radioname = $row['questionid'];
            @$user_id = $_SESSION['user'];
            @$userscore = $_POST[$radioname];

            if(@$_POST['submit_questionnair_btn']){
                $sql="insert into
userassessments(userid,questionid,score) values('$user_id','$radioname','$userscore')";
                mysql_query($sql);
                header("Location: home.php");
            }
        }
    }
?>
    END... <input class="btn btn-primary" type="submit"
name="submit_questionnair_btn" value="Submit Results"
onclick="return confirm('Ready to submit?'); " style="float:right;">
    </form>    </br></br></br></br>
</div>

<div class="footer"><?php include('footer.php');?></div>
<script src="assets/jquery-1.11.3-jquery.min.js"></script>
<script src="assets/js/bootstrap.min.js"></script>
</body>
</html>

```

*****Recommendation*****

```
<?php
    ob_start();
    session_start();
    require_once 'dbconnect.php';

    // if session is not set this will redirect to login page
    if( !isset($_SESSION['user']) ) {
        header("Location: index.php");
        exit;
    }
    // select loggedin users detail
    $res=mysql_query("SELECT * FROM users WHERE userId=".$_SESSION['user']);
    $userRow=mysql_fetch_array($res);
?>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Welcome - <?php echo $userRow['userName']; ?></title>
<link rel="stylesheet" href="assets/css/bootstrap.min.css" type="text/css" />
<link rel="stylesheet" href="style.css" type="text/css" />
<link rel="stylesheet" href="assets/css/crui.css" type="text/css"/>
</head>
<body style="overflow:hidden"><br>

<div><?php include('header.php');?></div> </br></br>
<div><?php include('sidemenu.php');?></div>
<div style="margin-left:15.5%;color:green;font-family:arial;font-size:18px;text-align:center">
    <span class="glyphicon glyphicon-bell" id="blink" style="font-weight:bold; color:red">
YOUR RECOMMENDATIONS </span>
    <p></p>
</div>
<div style="position: absolute; margin-left:15.5%; height:69%; width:83%; overflow-y: scroll;
border:1px solid #002F3F; border-radius:6px;">
    <?php
        include_once 'dbconnect.php';
```

```

//Retrieve Recommendations from the database
@$user_id = $_SESSION['user'];
//$user_id = $_SESSION['usr_id'];
$sql = "SELECT a.questionid,a.category,b.score AS YourScore,a.recommendations
FROM assessmentquestions a INNER JOIN userassessments b
ON a.questionid=b.questionid WHERE userid=$user_id and b.score<a.threshold";
//and assessmentdate>= CURDATE() ORDER BY a.questionid,c.category";
$result = mysql_query($sql);
$json = array();
if (mysql_num_rows($result) > 0) {
    // output data of each row
    echo "<table class='table table-hover'>
        <tr style='background:menu;'>
            <th>QId</th>
            <th>Category</th>
            <th>Score</th>
            <th>Recommendation</th>
        </tr>";
    while($row = mysql_fetch_assoc($result)) {
        $test_data[]=$row;
        $json['responses']=$test_data;
        $radioname = $row['questionid'];
        echo "<tr>";
        echo "<td id='radiobutton'>" . $row['questionid'] . "</td>";

        echo "<td>" . $row['category'] . "</td>";
        echo "<td id='radiobutton'>" . $row['YourScore'] . "</td>";
        echo "<td>" . $row['recommendations'] . "</td>";
        echo "</tr>";
    }
    echo "</table>";
    echo "<hr>";
}
else {

```

```

        echo "</br></br><p id='blink'>You are fully ready for Cyber Security; Therefore you
have no recommendations!</p>";
        echo json_encode($json)
    }
    ?>|
</div>
<div>
    <a href="#" class="btn btn-primary" role="button" style="position:
absolute;bottom:8%;margin-left:77%;" >Download Recommendations</a>
</div>
<div class="footer">
    <?php include('footer.php');?>
</div>
    <script src="assets/jquery-1.11.3-jquery.min.js"></script>
    <script src="assets/js/bootstrap.min.js"></script>
</body>
</html>
<?php ob_end_flush(); ?>

```