2021

A Framework for secure medical records: a case study of Kenyatta National Hospital.

Otieno, Theodulus Odhiambo
Faculty of Information Technology
Strathmore University

A FRAMEWORK FOR SECURE MEDICAL RECORDS

A Case Study of Kenyatta National Hospital

Theodulus Odhiambo Otieno

Master of Science in Information Technology

2020

A FRAMEWORK FOR SECURE MEDICAL RECORDS

A Case Study of Kenyatta National Hospital

Theodulus Odhiambo Otieno,

Submitted in partial fulfilment of the requirements for the Degree of

Master of Science in Information Technology at Strathmore University

Faculty of Information Technology

Strathmore University

Nairobi, Kenya

June 2020

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Theodulus Odhiambo Otieno

Signature…….....

Date…….....

Approval

The thesis of Theodulus Odhiambo Otieno was reviewed and approved by the following:

Dr Joseph Sevilla
Faculty of Information Technology
Strathmore University

Dr. Joseph Orero
Dean, Faculty of Information Technology
Strathmore University

Bernard Shibwabo, PhD
Director of Graduate Studies
Strathmore University

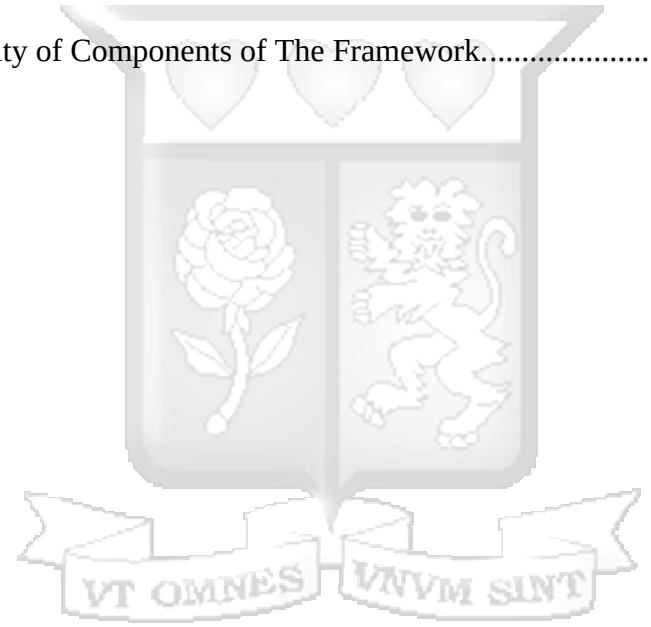
Abstract

Healthcare information systems are largely viewed as the single most important factor in improving healthcare quality and reducing related costs. However, managing Information Security is becoming more challenging because of security incidents due to non-compliance by health workers. This was an intrinsic case study to gain a better understanding of how a medical institution can embed information security culture in the management of security of its medical records. The application of case study research is appropriate in a new and emerging area of research as it a strategy that allows for an in-depth exploration of the phenomenon. A survey questionnaire was given to the employees of the Ear Nose and Throat department of Kenyatta National Hospital to measure the human aspects of the Information Security Program. Interviews were used to further explore the perceptions of respondents and probe for more information and clarification of answers. The study shows that management support, training and awareness, well-articulated and visible security policies will have a significant positive effect on compliance and hence the security of medical information. Additionally, the study showed that the employees have a great sense of commitment towards protecting the information of the organisation. This is because the management has taken the initiative to lead by example, avoids punishing workers for non-compliant behaviour and motivates the employees towards a security-conscious behaviour. This study sought to explore how the human factor may influence information security and how this can be harnessed together with technology to improve the security of medical records.

KEY WORDS: human factor, information security culture, electronic medical records, information security training, information security awareness.

Table of Contents

List of Tables



List of Figures

List of Abbreviations/Acronyms

COBIT - Control Objectives for Information and related Technology

EHR – Electronic Health Record

EMR – Electronic Medical Record

ENT – Ear, Nose and Throat

HIPAA - Health Insurance Portability and Accountability Act

IT – Information Technology

KNH – Kenyatta National Hospital

SPSS - Statistical Package for Social Sciences

WHO – World Health Organisation

Acknowledgement

Research and the writing of a thesis is not something one can do alone. This dissertation is an effort in which many people have contributed to. I want to express my heartfelt gratitude to all of them for their generous support.

I thank the Almighty God for giving me the energy and wisdom I desperately needed to complete this task.

My gratitude goes to my mentor and supervisor Dr Jose' Luis Sevilla whose critique and guidance helped me prepare this final draft.

My sincere gratitude goes out to Mr Mbatha of KNH for his support during the period of this study, Mr. Oyieyo for his valuable input during the last phase of this study and Dr Lizyben Chidamba of University of Pretoria, for his encouragement and support during the period of writing this dissertation.

I am grateful to my supportive family for urging me to complete this mountainous task.

Dedication

To my wife Nancy and our children Timothy, William and Wynnelle.

Chapter 1 Introduction

1.1 Background to the Problem

There is little doubt that Healthcare Information Systems (HIS) will move towards a fully integrated electronic medical record, EMR (Cheng et al., 2010). No doubt Kenya has initiated the development of its electronic health management systems with the aim of migrating paper-based records to the electronic form of records management (Ayieko, 2016). In 2012, the Kenyatta National Hospital (KNH) completed the digitisation of the records of its Ear, Nose and Throat (ENT) department. The new records management system was expected to improve the operations at the unit (The Standard, 2012).

Before the digitisation of records at KNH, "anyone could go to medical records registry and get access to the patient file. With digitisation of the patient medical file access will be allowed to specified users who must have a username and a password," (The Standard, 2012). However, as we move closer to a paperless environment and Internet-based applications, we must realise that the risks to privacy and security incurred by using electronic systems are also increased. This becomes a complex issue since social issues need to be considered as well as technological advancements to achieve a balance between public interests and personal privacy (Cheng et al., 2010).

Anecdotal evidences from recent years also suggest that a lack of adequate security measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish and possible social stigma (Appari and Eric,2010). Therefore, to prevent data breaches, healthcare organisations need to adopt suitable safeguards. Such measures involve a mix of employee training, smart use of technology and physical security for buildings. These measures can be taken from both an administrative and technical point of view (Daily Nation, 2020).

Acuña (as cited in Glaspie, 2018, p1) argued that an organisation's investment in just technology does not eliminate the many security challenges, it is well known that humans are the weak link in information security. Van Niekerk (2010) opines that humans, at various levels in the organisation, play a vital role in the processes that secure information resources. They further suggest that the problems experienced in information security can be directly contributed to the humans involved in the process. One approach towards addressing the

behavioural aspects of the human factor in information security is to foster an organizational sub-culture of information security (van Niekerk, 2010).

Within an organisation, culture manifests itself by considering values, behaviours, attitudes, actions, management related activities and physical environment (Salahuddin-Alfawaz, 2011). Öğütçü, et al., also posited that an end-user's undesirable behaviour is a direct reflection of the culture of information security in the organisation (as cited in Glaspie, 2018, p1). From the foregoing, it then becomes clear that the human factor, whether intentional or due to negligence can be a great risk to information security.

1.2 Problem Statement

With the advances in security technologies, many computing behaviours are now being automated to reduce the task knowledge and time burdens on end users. However, behaviours such as appropriate use of computer and network resources, appropriate password habits etc., that cannot be addressed by security technologies are often dealt with through organisational computer security policies (Herath and Rao, 2009). According to a recent article (Davis, 2019), in 2018, the healthcare sector saw 15 million patient records compromised in 503 breaches, three times the amount seen in 2017, according to the Protenus Breach Barometer. But just over halfway through 2019, and the numbers had skyrocketed with potentially more than 25 million patient records breached. In addition, a report by IBM indicated that 9 out 10 security breaches were as a result of some kind of human error (as cited in Glaspie, 2018, p1).

The risk that employee's behaviour poses to the protection of information assets is one of the primary motivations for focusing on cultivating an acceptable information security culture. Therefore, a multi-faceted approach towards information security management could empower end-users and the management in the quest to improve the security of medical records. Specifically, a socio-technical framework is the intended output of this study.

1.3 Aim of the Study

The aim of this study is to explore how the human factor may influence information security and how this can be harnessed to improve the security management of medical records.

1.4 Research Objectives

The objectives of this research were to:

1. Examine the human factors that currently constitute or reflect information security culture.
2. Examine the state of information security culture at Kenyatta National Hospital.
3. Design a framework that would ensure better security management of Electronic Medical Records.
4. Validate the information security framework.

1.5 Research Questions

In order achieve the research objectives; the following research questions were constructed:

1. What factors currently constitute or reflect information security in organisations?
2. What is the state of information security culture in medical institutions in Kenya?
3. What should an information security framework comprise of to provide better security for medical records?
4. Does the proposed framework ensure better security of medical records?

1.6 Justification and Significance of the Study

Electronic Medical Record (EMR) systems are increasingly being adopted in Kenya to improve the management of medical records, health program management, and the quality of patient care. It is anticipated that the proposed framework will ensure better security of medical records and that the outcome of this research will also be relevant to other medical institutions in their quest to develop and deploy an information security culture. It is also anticipated that the outcomes of this research will provide a sound basis towards further research into information security management in medical institutions in Kenya.

1.7 Scope, Limitations and Assumptions

1.7.1 Scope

Kenyatta National Hospital (KNH) has embarked on digitising some of it medical records of the Ear, Nose and Throat (ENT) clinic. The study will target security of electronic medical records at the ENT clinic and will therefore be limited to the medical personnel at the clinic, clerks and senior managers at the records department. The nature of the objectives of the study will restrict the study to those users who may have authority to access medical records from time to time.

1.7.2 Potential Limitations

Some of the limitations affecting this study include:

i. Information security culture is a relatively new concept of research
ii. Analysing human factors is a complex task since human factors are subjective in nature and depend largely on the specific context of the organisation.
iii. Lack of support and understanding of importance of academic research by the target population.
iv. Companies view Information Security as company secret and may not be willing to disclose much.

1.7.3 Assumptions

The following assumptions will be made during the study that:

i. there are people who are interested in information contained in medical records stored by KNH.
ii. the behaviour of employees handling medical records at KNH is a threat to the security of medical information.
iii. the research findings will be applicable to other departments within KNH and health institutions in Kenya.

Chapter 2 Literature Review

2.1 Introduction

The purpose of this chapter is to provide an understanding of human aspects and how they influence information security culture. This chapter presents the literature review of academic and professional literature on information security culture. The chapter will be concluded by identifying model factors that conceptualise security culture. The chapter starts with the concept of information security.

2.2 Information Security

Every organisation must have Information security, to protect the *Confidentiality*, *Integrity* and *Availability* of information assets, whether in storage, processing, or transmission. This is achieved via the application of *Policy*, *Education*, *Training and Awareness*, and *Technology*. (Whittman and Mattord, 2011). Information security includes the broad areas of information security management, computer and data security, and network security. This is illustrated in Figure 2.1.

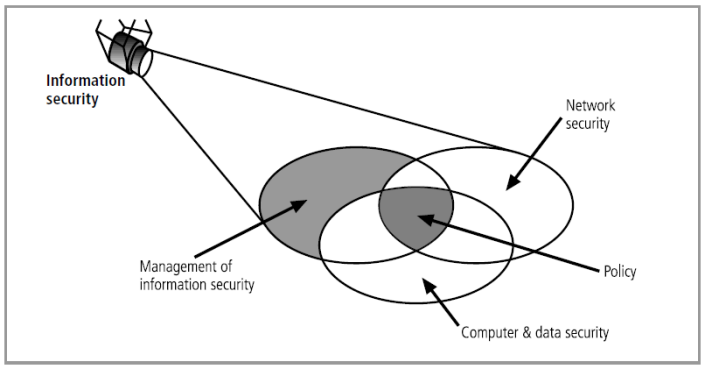


Figure 2.1 Components of Information Security.

(Source: Whitman, 2011)

Information security may also be defined as “the prevention of, and recovery from, unauthorised or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional” (Al Natheer, 2012).

2.3 Organisational Culture

Organisational culture is "a system of shared meaning held by members, distinguishing the organisation from other organisations". According to Manetje (2009), "organisational culture is the distinctive norms, beliefs, principles and ways of behaving that combine to give each organisation its distinct character". These will inform the way the organisation will cope with the problems associated with its internal integration and external adaptation. Organisational culture exists on three different levels (Schein, 2004). This is illustrated in Figure 2.2.

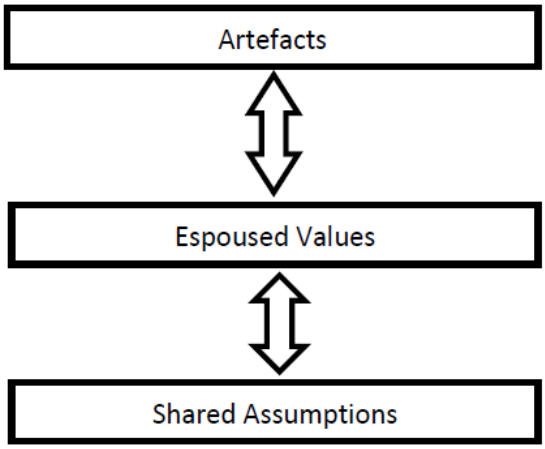


Figure 2.2 Levels of Culture

(Adapted from Schein, 2004)

1. Artefacts include the behaviour of members of the culture (Schein, 2004).
2. Values in organisations are the social principles, philosophies, goals, standards and beliefs considered to have intrinsic worth for members of the organisation. Teamwork and the belief that everyone is important in the decision-making process are typical espoused values (Van Niekerk and Von Solms, 2010).
3. Assumptions represent taken-for-granted beliefs about reality and human nature. These are elements like routines, which form an important part of an organisation's culture (Fagerström, 2013).

Van Niekerk and von Solms (2006), suggested that if an organisation were trying to foster a subculture of information security, all activities would have to be performed in a

way that is consistent with good information security practice. However, this change requires the unlearning or modifying of the employees' current beliefs (Fagerström, 2013) but due to human nature, this change might face a lot of resistance. For this to be successful, adequate knowledge regarding information security is necessary.

2.4 Human Behaviour and Culture

Human beings are rational, their behaviour and the choices they make are partly guided by their intensions (Aurigemma and Mattson, 2017). More specifically, individual choices and behaviours are determined by their state of mind (personal attitude), social pressure from others (subjective norms), and a sense of control. Agreeing with this, Bulgurcu et al., (2010) postulates that an employee's intention to comply with the organisation's Information Security Policies is influenced by subjective norms (social pressures from other), perceived behavioural control, and attitude toward compliance. However, an organisation's hierarchy with respected command and control structures might impact how much control an individual has over a set of behaviours, adds Aurigemma and Mattson (2017). Considering this issue, Herath and Rao (2009) acknowledge that social pressure may have an effect on an employees' behaviour and therefore creating a culture or an environment that fosters security is a good strategy. Every cultural setting has particular values, beliefs and practices but values, beliefs and attitudes significantly affect the behaviour of individuals (Hadjor and Gadasu, 2014). Values are goals and motivations that serve as guiding principles in an individual's life Myyry et al., (2009). A person's value priority plays an important role in how they behave and how they make decisions.

2.5 Information Security Culture

The following introductory ideas set the scene for a better understanding of the concept of information security culture:

Information security may not always be wholly technical or wholly social but most definitely be a combination of both. Technology elements may involve a combination of cryptography, intrusion detection systems, access control mechanisms, firewalls, antivirus, and so on (Tarimo, 2006). Management elements can be access control policy or a general

security policy, procedures and practices. Social elements involve, in addition to the management elements, —ethical/cultural, and legal/contractual issues (Tarimo, 2006).

These elements can be grouped into two major categories of technical and social controls. The attitudes and behaviours of the people who interact with the system also contribute to the overall effectiveness even of the most comprehensive security system (Tarimo, 2006). The overall range of security requirements for an organisation determines the nature of ICT security culture that is to be cultivated. In addition, the same security requirements determine the policy and types of countermeasures (security system) to be implemented. Furthermore, the security requirements impose demands on the people who would interact with the system. This is illustrated in Figure 2.3.

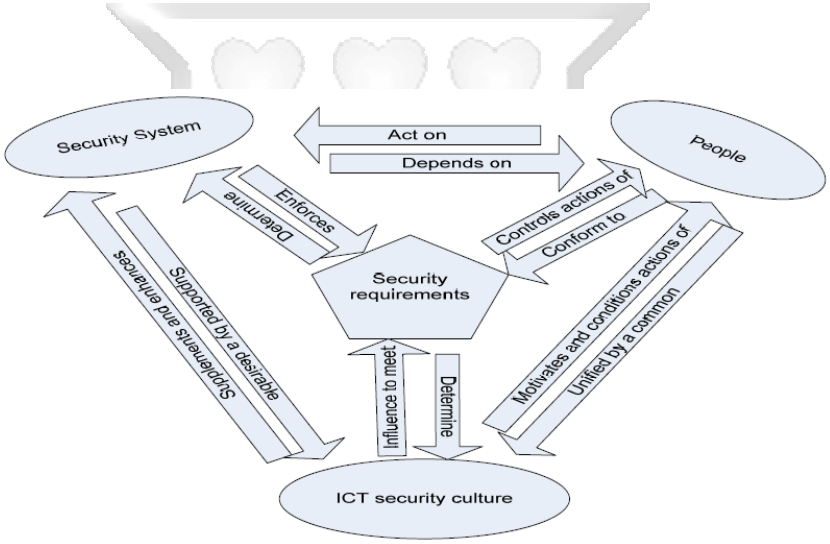


Figure 2.3 ICT Security Culture in Relation to Other ICT Security Controls.

(Source: Tarimo, 2006)

2.5.1 Defining Security Culture

There seems to be no single and clear definition of Information Security Culture. However, it is possible to infer the ways in which information security culture manifests itself in an organisation by considering values, behaviours, attitudes, actions, management related activities and physical environment (Salahuddin-Alfawaz, 2011). The manifestations of security culture are represented in Figure 2.4.

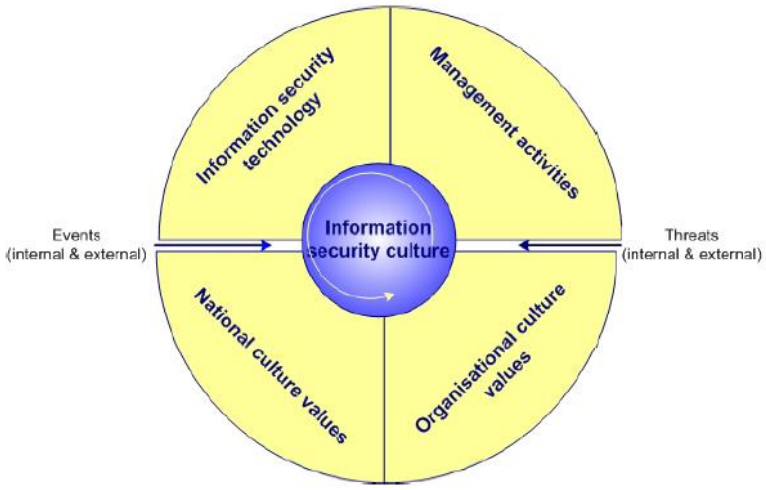


Figure 2.4 Manifestations of Security Culture.

(Salahuddin-Alfawaz, 2011)

2.6 Information Security Policies

Effective information security management can only be predicted on the existence and execution of an information security policy. Without a policy, security practices will be developed without clear demarcation of objectives and responsibilities (Fulford, 2003). Security policies are put in place to communicate conventions and assign clear roles for employees and acceptable behaviour during the execution of their duties (Bulgurcu, Cavusoglu, & Benbasat, 2010). Information security policies and procedures should be clear and understandable for staff (Safa et al., 2015). When they are clearly defined, policies influence and determine employees' course of action (Herath and Rao, 2009). Such a policy can be supported by a hierarchical system of sub-policies and procedures outlining various lower-level controls (van Niekerk, 2010). An organisation must have a comprehensive information security policy for it to have an impact on the security culture. Such a policy must be backed by appropriate technology systems and a security culture (Acuña, 2016). However, having a security policy alone cannot ensure employee compliance. Human knowledge also plays a key role in behaviour change which will influence an employee's intentions to comply with information security policies (Safa et al., 2016).

Additionally, an individual is less likely to be involved in deviant behaviour if they have a strong attachment, commitment and involvement in the conventions of the

organisation. They are therefore less likely to deviate from the organisations policies (Safa, Von Solms and Furnell, 2016). Therefore, management must take an active role in motivating employees towards policy compliance (Glaspie, 2018). A study by Han, Kim, & Kim (2017) reported that employees are more likely to comply with information security policies if they recognise the benefits of information security policy compliance. This is further supported by van Niekerk (2010), who suggested that employees must be motivated to behave in a way that would promote security compliance. A study by Ifinedo (2013) posited that information security compliance is affected by social attributes like bonding and influence. Social bonds formed at work largely influence attitudes formed towards compliance. There is therefore a need to integrate the social component as a factor influencing the intention to comply with the information security policy.

2.7 Training and Awareness

Training and awareness is the foundation of any information security culture. It provides employees with the required knowledge of their roles and expectations regarding their specific operational controls in the matters of information security (van Niekerk, 2010). Further to this it is worth noting that lack of relevant information security knowledge amongst organisational end-users could compromise the security of information assets. It is vital that organisations ensure that the humans in the information security process have the requisite information security knowledge.

Price Waterhouse Coopers reported that a security awareness and training programme is critical to ensure the success of an information security programme (as cited in da Veiga and Martins, 2015, p3). Users are likely to disregard a security control if they feel that it is interfering with their way of getting things done. Management can address this by not only educating employees about their information security roles and responsibilities, but also by addressing the underlying factors which could influence their behaviour (van Niekerk, 2010). Training plays an important role in cultivating a culture (von Solms, 2004). The target with information security training is to make the employees act according to the management wishes so that the company's information is properly protected. However, employees do not need to know everything about information security, but they must be

informed about the associated risks and how they can minimise these risks (Fagerström, 2013).

A strong information security culture provides significant protection to information assets of the organisation. It minimises employee-related risks and enhances compliance with information security policy (da Veiga and Martins, 2015). A study by Parsons, McCormac, Pattinson, Butavicius, and Jerram, (as cited in Glaspie, 2018) reported that businesses often leave employees poorly trained or not trained at all while investing heavily on software and hardware. As a result, the employee becomes a very big security risk to the organisation whereas the end-users who possess the adequate knowledge of information security concepts are more comfortable in their use and can contribute to the security awareness program through knowledge sharing.

2.8 Management Support

Management support is a critical success factor in the cultivation of an information security culture van Niekerk (2010). Top management support is crucial in creating a supportive environment in the organisation and providing the necessary support which includes sufficient budget allocation, setting an example, and human capital. This support is a necessity in that it creates a participatory environment by the employees which leads to the achievement of an organisational information security culture. Such participation and commitment by management aids in establishing a structured approach to transforming teams, individuals and the entire organisation to handle information in line with the organisation's information security policies (Da Veiga and Martins, 2015).

The management must disabuse the perception that information security is the responsibility of the IT department, who should ensure that all the technical controls and software are adequate to ensure the security of the organisation's resources. Additionally, senior management must be fully behind the implementation of the organisation's information security culture (Alavi, 2016). Changing the prevailing corporate culture requires the unlearning or modifying of the employees' current beliefs. Due to human nature, this change might face a lot of resistance. The most influential factor on employee beliefs and attitudes is the working environment, which is why the change culture must originate from the senior management (Fagerström, 2013). A study by da Veiga and Martins (2015),

suggested a need to embed an information security culture where the interaction of employees with information assets contributes to the protection of these assets. Top management must continually monitor and influence the behaviour of employees in compliance with information security.

A study by Aurigemma and Mattson (2017) suggests that the hierarchy of employees in management positions has a significant impact on the information security attitudes and behaviours of others. Since they influence behaviours, management must have a deep understanding of a company's business processes and how any design or changes will affect the information security (Glaspie, 2018).

2.9 Sanctions and Rewards

Rewarding desirable behaviour and punishing undesirable behaviour are both vital factors in shaping employee compliance in information security. Training can help to change behaviour but must also be supported through the proper positive and/or negative incentives, as well as strong leadership (van Niekerk, 2010). The perceived threat of sanctions influences personal behaviours through the certainty and severity of punishment, i.e., as punishment certainty and punishment severity are increased, the level of illegal behavior should decrease (Herath and Rao, 2009). They further suggest that auditing mechanisms are a good deterrent measure for deviant behaviour. It is expected that with higher awareness of existing detection mechanisms in a workplace, employees are more likely to comply with the security policies. Which results in a healthier information security culture.

However, instead of using deterrent measures, Kabay (as cited in van Niekerk, 2010, p66) suggests that employees should be praised for exhibiting the correct information security behaviour as this will result in a better response towards compliance. Kabay further suggested that a change of attitude can also be achieved by using persuasion. Some other studies also agree that sanctions and formal punishment may not be the best approach towards achieving information security compliance. D'Arcy, J., & Devaraj, S. (2012) suggest that a predisposition toward the need for social approval and moral beliefs regarding the behaviour are key determinants of technology misuse. This demonstrates that moral beliefs and social pressures are considered when employees make compliance decisions.

A study by Hu, Xu, Dinev, and Ling (2011) suggested that deterrence has no influence on an individual's intention to comply with information security policy. Hu et

al., further stated that perceived benefits and intrinsic satisfactions are more influential in compliance decision making. Additionally, top management must commit in terms of resources to enable rewards for desirable behaviour, and in terms of authority to allow the punishment of undesirable behaviour, Alpander & Lee (as cited in van Niekerk, 2010, p218).

2.10 Security Ownership

When top management is committed to information security and espouse this commitment through policies and procedures, a culture of information security will exist in which user will want to behave in a secure manner (van Niekerk, 2010; Corris, 2010). It is also important that management demonstrate this commitment by rewarding employees who behave correctly. Additionally, management needs to promote an environment where employees have the attitude (the desire) to protect the information resources of the organisation (Corris, 2010).

An employee's attitude is influenced by how messages are contained in the body of knowledge, reports Box and Pottas (2014). When the message is one of motivation and explains the benefits and positive effects of compliant behaviour, the attitude of the user is changed from being compliant due to fear of punishment to one of being compliant because the message communicated in the body of knowledge is aimed at the user's sense of achievement. The employee the feels a strong sense of obligation and ownership towards the information security.

Another study (Ahlan, Lubis and Lubis, 2015) concluded that the intention of a security policy is to allow users to reflect, own their own terms, why security is important and how they should react in various circumstances. Ultimately the responsibility of whether to adhere to organisational security policies or ignore them is then left to employees, who may then choose to break security policies for malicious purposes or choose to evade security policies, for mere convenience (Herath and Rao, 2009). However, employee actions related to security policy compliance may also be difficult to monitor and so surveillance control techniques may be necessary in a workplace (Herath and Rao,2009). The major threat to information security is constituted by careless employees who do not comply with organisations' information security policies and procedures (Siponen et al., 2007).

2.11 The Kenyan Perspective

2.11.1 Introduction

Organisations are becoming increasingly reliant on information technology to fulfil many of their basic functions. The move to a digital economy has caused information and communication technologies (ICTs) to become valuable business assets that need to be protected (Makumbi et al., 2012). However, the (poor) attitude of employees towards information technology has negatively affected the adoption of information systems in public hospitals (Odiwuor et al., 2015).

2.11.2 Factors Influencing Implementation of Technology in Kenya

Kanyua (2015), records that the ministry of health has identified Information Communication Technology (ICT) as one of its reform strategies to ensure they effective service delivery toward vision 2030. Health information technology can improve administrative functions as well as reducing medical errors by enforcing clinical guidelines and reducing healthcare cost. For the successful implementation of information system in organisations, and to avoid adoption failure, the health institutions should provide employees with computer education and training courses.

Security Education

A study (Kanyua, 2015) found that many employees in the public hospitals do not have specialised information systems knowledge and are lacking in technical skills. This view is also supported by Odiwuor et al., (2015) who found that there was lack of capacity among healthcare providers to effectively and efficiently use ICT to bring meaningful impact in the quality of health services in Gatundu North. Further to this, they found that those workers who had some training in using information technology did not have training relevant to the healthcare industry. Additionally, a study by Kanyua (2015) also revealed that training could help medical professionals in their decision-making and improve delivery efficiency.

Budget

There is also a lack of sufficient budgetary support for IT security within most organisations. As a result, the organisations are installing sophisticated security measures without the presence of dedicated security personnel (Makumbi et al., 2012).

Security Threats

A study (Makumbi et al., 2012) revealed that system users especially disgruntled system users are a considerable threat to information assets of an organisation. They identified several threats to information and the countermeasure currently employed by some organisations. These are summarised in **Appendix E.**

Security of Medical Records

In their study on medical records system based in rural Kenya (Hannan et al., 2000) reported that none of the staff were familiar with the process of storing and retrieving information stored in a computer or other electronic system. It was therefore necessary that the staff undergo training on how to use the new system.

Other study by Lelei (2010), reported that medical research information at Kenya Medical Research Institute (KEMRI) is not secure. The medical information faces several threats from viruses and worms, data leakage by employees, intrusion and theft. General policies on information security are not well defined; they are not well documented nor are they communicated to employees in the organisation. The policies on information security are not easily accessible to employees and no policy exists regarding the medical research information. An interesting find by Lelei (2010) indicated that 60% of doctors and clinical officers had shared their passwords whereas 53.8% of lab technicians had equally shared their passwords.

2.11.3 Conceptual Framework

The overall effect of an organisation's information security culture can be seen to be an aggregate of the several underlying levels that underpin culture or human behaviour. Each of these can positively or negatively affect the information security culture. The conceptual framework illustrates the relationship between the variables used in the study and illustrates

the functional design of the framework. The conceptual framework is based on the outcomes of the reviewed literature.

The conceptual framework considers the human factors are variables that affect information security culture. We considered the independent variables as management support, training and awareness, information security policy, attitude and commitment, sanctions and rewards whereas the dependent variable is information security culture. The model is seen in Figure 2.5.

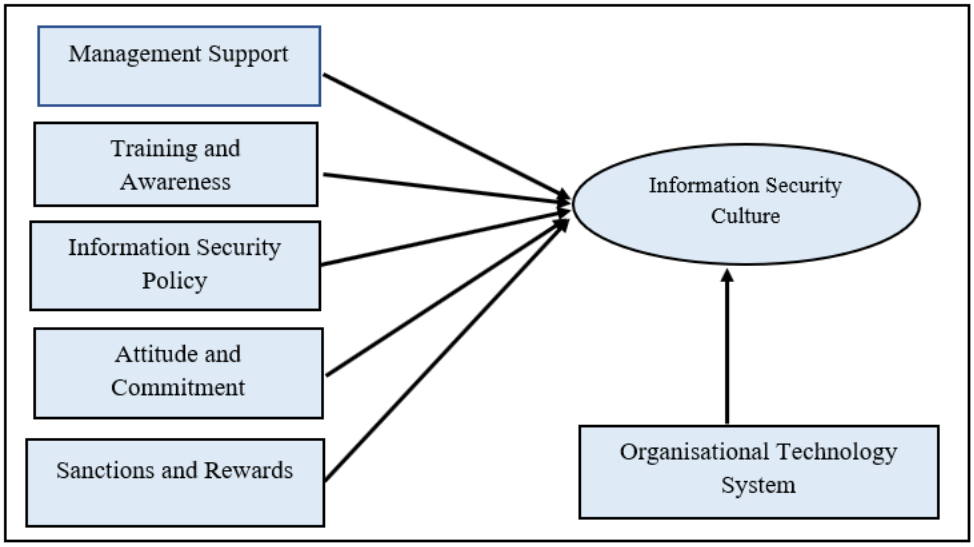


Figure 2.5 Conceptual Model.

2.12 Summary

This chapter presented a review of information security and information security culture. There is little clarification by the literature reviewed as to what factors may constitute security culture in a medical institution. Based on the literature reviewed in this study, the top ideas for conceptualising of security culture were:

- Training and Awareness.
- Management commitment.
- Attitude and Commitment.
- Security policy.
- Sanction and Rewards.

The literature also speaks to the idea that organisations in Kenya are aware of the security threats to their information assets. However, none of the literature has suggested how to address the human factor, which is a threat factor. In other words, there is a clear gap in knowledge in terms of what factors constitute information security culture in medical institutions in Kenya.

Therefore, the current study will take this initiative and determine what factors constitute security culture. To achieve this goal, an open-ended interview and a questionnaire was implemented to determine these factors at the ENT clinic.

Additionally, the qualitative interviews will also assist with developing a framework for ensuring the security of medical records. Other factors may also emerge after conducting and analysing the qualitative interview.

The outcomes of the qualitative analysis are presented in Chapter 4.

Chapter 3 Research Methodology

3.1 Introduction

Chapter 2 presented a critical review of the available literature to assess the human factors that would be the characteristic attributes of a successful information security culture. In addition, the study looked at how these factors could be harmonised into a security management framework for a medical institution. This led to a conceptual model as seen at the end of the previous chapter. The conceptual framework demonstrates how the human factors relate with information security culture and will eventually lead to the recommendation of a framework that would address these security needs at the ENT clinic.

The information, generated from the literature review, was used to develop the qualitative interview and the survey questionnaires. This chapter presents the design and methodology that were used in the research.

3.2 Design

Garring (2004) defined a case study as "… an intensive study of a single unit with an aim to generalize across a larger set of units." Yin (2003) has defined a case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident". A case study is also detailed by Neuman (2014) as a methodology that "intensively investigates one or a small set of cases, focusing on many details within each case and the context. In short, it examines both details of each case's internal features as well as the surrounding situation." Pable (n.d.) reported that a case study method permits in-depth, extended engagement with individuals, which may have extended advantages.

Aside from this, "The logic of the case study is to demonstrate a causal argument about how general social forces shape and produce results in particular settings." In addition, Stake (1994) identifies intrinsic case study, instrumental case study and collective case study as three types of case studies. An intrinsic case study aims at increasing the understanding of a phenomenon and make sense of the case being studied. Instrumental case study aims at

refining a theory. In a collective case study, a researcher aims at using several case studies to compare and draw general implications of the phenomenon being studied.

The research adopted an intrinsic case study approach to gain a better understanding of how a medical institution can embed information security culture in the management of its medical records. The application of case study research is appropriate in a new and emerging area of research as it a strategy that allows for an in-depth exploration of the phenomenon. Yin (2003) indicates that "Case study inquiry copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result benefits from the prior development of theoretical propositions to guide data collection and analysis".

Interview protocols and questionnaires were developed based on various factors that were identified in the literature.

The objectives of this study were:

1. Examine factors that currently constitute or reflect information security culture.
2. Examine the state of information security culture in Kenyan medical institutions.
3. Design a framework that would ensure better security management of Electronic Medical Records.
4. Validate the information security framework.

An in-depth review of available literature was carried out to determine the factors that currently reflect information security culture. Available literature from Kenya was reviewed to determine the state of security culture in Kenyan hospitals.

Through a qualitative study, the researcher was able to uncover employees' behaviour, perception and attitude towards information security matters that may affect the security of medical records. The research design links the data collected, and conclusions drawn to the initial questions of the study. It therefore, provides a conceptual framework and a plan of action of how to get from questions to a set of conclusions.

3.3 Population and Sampling

The study employed purposeful sampling. According to an article (Benoot, Hannes, and Bilsen, 2016) it was reported that:

> "The logic and power of purposeful sampling lie in selecting information-rich cases for study in depth. Information-rich cases are those from which one can learn a great deal about issues of central importance to the purpose of the inquiry, thus the term purposeful sampling. Studying information-rich cases yields insights and in-depth understanding rather than empirical generalizations."

We selected the ENT department of KNH which is implementing Electronic Health Records in the management of medical information. Participants were selected from senior management and employees who are involved in accessing patient records and storing them. The total number of participants were 35 as shown in Table 3.1.

Table 3.1 Number and Category of Respondents

Category	Number
Doctor	9
Nurse	8
Lab Technician	5
Records	9
Managers	4
Total	35

3.4 Data Collection

Data was collected using survey questionnaires and semi-structured interviews with the focus group.

3.4.1 Questionnaire

Questionnaires provided a cost-effective way of gathering information given the nature of the study. It provided anonymity where sensitive questions were asked and therefore promoted the chance of more honest answers.

Based on the literature reviewed and the goal of the study a conceptual model was constructed. Measuring the security culture was based on information security program and the culture at Kenyatta National Hospital specifically at the ENT clinic. We then designed a questionnaire that sought to investigate the prevalence of these factors at KNH. These factors were investigated by questions in the instrument.

The questionnaire sought to elicit specific information in relation to the medical records based at the ENT clinic. The purpose of these questions was to establish the role of the interviewee with respect to information security measures. The outcome of the interviews and the questionnaires will assist in identifying factors that reflect information security culture, and factors driving information security culture in the context of the ENT clinic.

The questionnaire was designed with three major sections:

- Section I: gathered demographic information about the respondents.
- Section II: gather information will elicit respondents' opinion on factors that would influence security culture at KNH.
- Section III: To obtain respondents' opinion about security culture concerning security policy, security awareness, security training and security compliance.

Since cultural aspects are qualitative, the attributes were measured by questions that sought the opinions and perceptions of the respondent regarding an aspect of culture. The process is explained here:

a) Top management support

Management support reflects the organisational commitment to information security and the importance attached to information security awareness. The moment employees feel that their management is not paying attention to information security, it will be reflected the security culture of the organisation. Five questions in the survey instrument measure the user's opinions on their management's involvement in the overall information security of the organisation. For example: "Senior management is always involved in key information security activities."

b) Information Security Policy

Policies are not useful if employees do not know of their existence or if they exist but are not accessible. The instrument has four questions that talk to policies as they relate to information security and whether the employees are aware of them. For example: "There is a clear procedure to discipline members who violate organisational security policy and regulations."

c) Information Security training and Awareness

This factor addressed the training and overall understanding of the sensitive nature of the data handled by the employee during their work. An example of a question in this category is: "do you think information security related behaviours of members of your organisation can be influenced by managerial security initiatives like policies, guidelines and training programs?"

d) Attitude and Security Ownership

This refers to the employee's overall attitude towards the information security program and their involvement in protecting company's assets. An example of a question in this category is: "It is my responsibility to protect the information of my organisation."

e) Sanctions and Rewards

An organisation must have the ability to prevent or control the behaviour of an employees through fear of some penalty or some form of punishment. Questions were asked which defined how the respondent perceives that the organisation controls their work-related activities. For example: "There is a clear procedure to discipline members who violate organisational security policy and regulations."

The questionnaire is attached in **Appendix A**

3.4.2 The Semi-Structured Interview

The interviews will be used to explore the perceptions and opinions of respondents regarding complex and sometimes sensitive issues and enable probing for more information and clarification of answers. The interview schedule is attached in **Appendix B**

3.5 Testing and Validating Instruments

A draft questionnaire was pre-tested to ensure the questions were understood by the respondents and there were no problems with the wording of the instrument. A select group of 22 Master of Science in Information Technology (MSIT) were used to pre-test the questionnaire. Based on the comments made from the pre-test, a few modifications were made to the questions to improve their clarity before using them in the actual administration of the questionnaire and the interview process.

3.6 Data Analysis and Presentation

Data Analysis

Raw data collected was subjected to coding before it was analysed. All of the questions outside of the demographic section were operationalised in a 6-point Likert scale with the range of: Strongly agree, Agree, No idea, Disagree, Strongly disagree, Not Applicable. The research utilised descriptive statistical data analysis using Statistical Package for Social Sciences (SPSS), Pallant (2010). The descriptive statistics produced frequencies and graphs for qualitative results.

Presentation

Several graphical tools were used to represent the data including bar graphs, tables and pie charts.

3.7 Designing the framework

The information security culture framework was developed based on the outcome of the literature review and the qualitative interviews.

A concept map of the factors driving security culture, how this reflects in an organisation, was developed based on the findings of the investigation. This was then refined into the proposed framework.

3.8 Validating the Framework

Information security is not purely a technical issue but must involve the employees as well. A comprehensive framework is important to ensure all the factors pertaining to

information security are covered. To validate the framework, the researcher used the outcomes of the survey before the framework was implemented as a benchmark. After the implementation of the framework, a second survey was done to measure the effect of the implementation of the framework on the state of information security culture. This survey was done using an online using google form. The survey questionnaire used in the survey is available in **Appendix D.**

Thirty-five participants were invited to the online survey to review the components of the proposed framework in relation to the outcomes of its implementation. Their feedback was collected and analysed using SPSS to validate each component of the proposed framework. Each component was translated into several statements that represented the component. A total of twenty-three items were formulated. A ranking scale was used to evaluate and indicate the level of importance of each task (Table 3.3). A score of 0 – 5 was used to rate the response with zero meaning not applicable to five meaning highly important. Figure 3.1 shows an extract from the survey.

Table 3.2 Survey Scale

N/A	Very Low	Low	Average	High	Very High
0	1	2	3	4	5

Figure 3.1 Extract of the Survey

3.8.1 Internal Consistency Reliability

To assess whether the twenty-three items that were summed to constitute a security culture construct were reliable, Cronbach's Alpha was computed. For a model to be valid and practical, it must be reliable (AlHogalil, 2015). Cronbach's alpha, a coefficient of internal consistency, was used to measure reliability, providing an indication of how consistent the responses were across items within the scale. Cronbach's alpha values must meet the minimum accepted criteria (above 0.7) to confirm the consistency and reliability of the framework (Da Veiga et al., 2007).

3.9 Summary

This chapter presented the methodological approach employed by the research project. First, it discussed the introduction, research design, and the justification for the research design. The research approach employed was qualitative. It also discussed a method that will be used to test the validity of the theoretical framework.

Chapter 4 Presentation of Research Findings

4.1 Introduction

This chapter contains presentation and analysis of all the qualitative data collected from interviews of several users and stakeholders of the medical records at the ENT clinic as part of this dissertation. The questionnaire is attached in **Appendix A.**

4.2 Data Analysis

The data collected from the questionnaires was coded into the various constructs that constitute (reflecting and driving) information security. The analysis of this data was then done using SPSS. The research question aimed at identifying the human factors that were playing out at KNH and that are likely to influence the cultivation of a security sub-culture for information security management. To understand the information security culture in an organisation, we must first understand its information security environment, practices and issues. Using a semi-structured interview, the participants responded to questions concerning ENT clinic's actual practices.

4.2.1 Threats to information security

From the observations made, the medical records at the ENT clinic face major threats the largest threat being attributed to users. The observations are summarised in Fig 4.1. The second factor they selected can easily be tied with the first one. This is the case of viruses and malicious software. The third factor listed was hardware failure, which may point to either lack of proper skills among the IT staff or lack of information security staff.

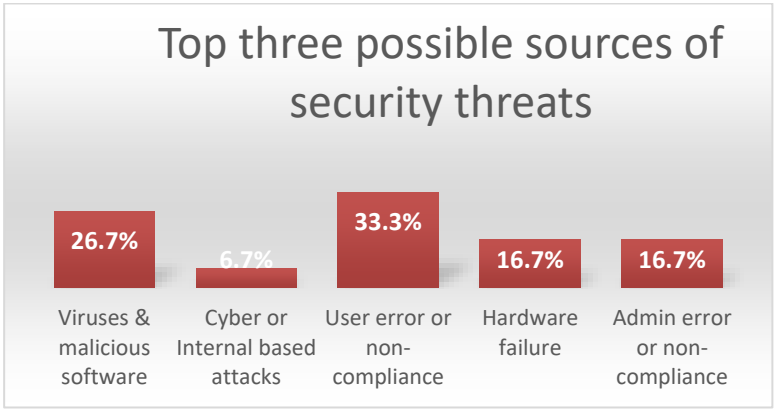


Figure 4.1 Top Three Sources of Security Threats

4.2.2 Top Management Involvement

As seen earlier in section 2.15.2, Information Security Management experts agree that top management commitment and involvement in information security is considered as an important factor in improving or creating a security culture. The results of this study agree with this as indicated in Figure 4.4. Considerations of this factor will therefore be included in the suggested framework.

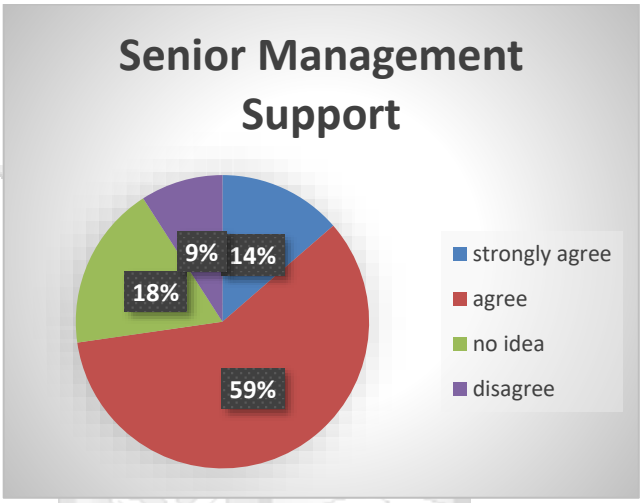


Figure 4.2 Top Management Support to the Security Program

Senior leadership must understand the importance of information security function. They must be involved in defining and communicating security policies and allocating specific responsibilities to different people. This is reflected in Figure 4.3

Figure 4.3 Management Ensures Decision Makers are Accountable for their Decisions and Actions.

The employees of KNH have indicated, as shown in Figure 4.4, that senior management is an essential part in the establishment of a security culture. This initial support is necessary if long-term success is to be envisaged.

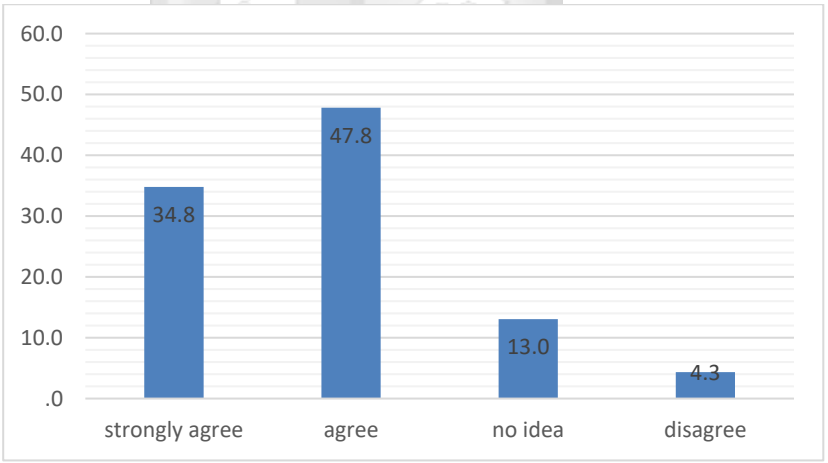


Figure 4.4 Top Management Considers Information Security an Important Organisational Priority.

4.2.3 Information Security Compliance

The respondents were asked to choose top three barriers to Information Security compliance. Figure 4.5 shows their responses. Majority of them feel that lack of adequate technology is the greatest barrier to compliance. It is quite interesting that none of the respondents mentioned anything to do with personal values and beliefs.

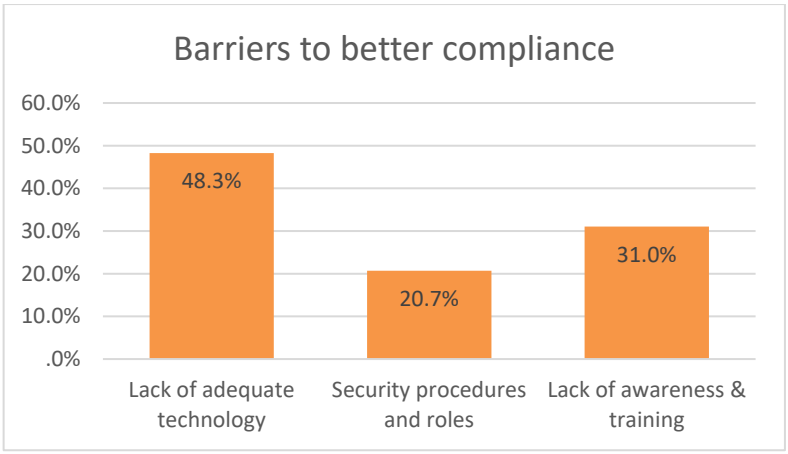


Figure 4.5 Top Three Barriers to Security Compliance

This was followed by lack of awareness and training programs. In the third place was lack of proper procedures and roles.

4.2.4 Adherence to Information Security Policy

Most of the respondents also felt that they and others around them, adhered to information security policy as seen Figure 4.6 and Figure 4.7

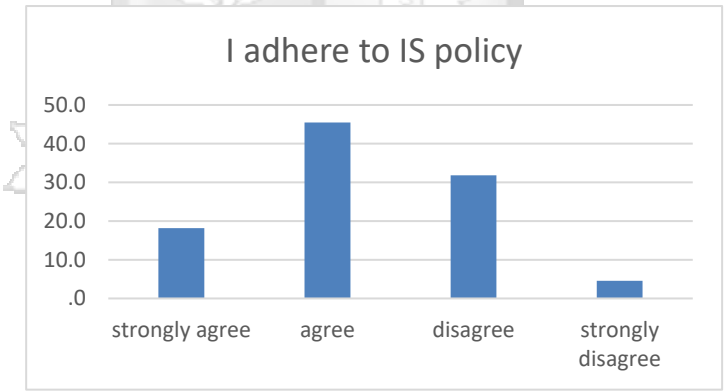


Figure 4.6 Adherence to Information Security Policy

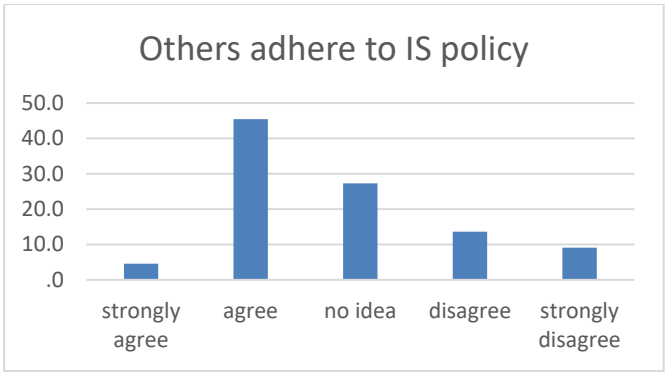


Figure 4.7 Others Adhere to Information Security Policy.

4.2.5 Information Security Policy

Information-security policy maintenance has been found to be a key factor that must be considered in the formulation of a security culture. Figure 4.8 indicates that there is lack of clearly defined policies within the organisation. A security policy is of great importance if there is a need to change staff security behaviour of culture as seen in section 2.16.4.

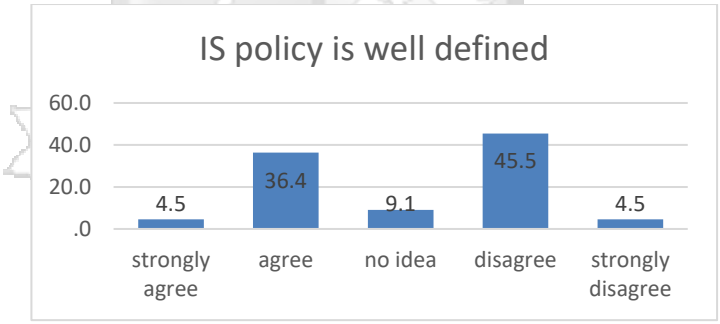


Figure 4.8 Information Security Policy Clearly Defined.

4.2.6 Sanctions and Rewards

At the time of the study, it appeared there was no comprehensive information security policy in place. However, it appears information security policy is embedded in the hospital's overriding ethos and policies as indicated by Figure 4.9.

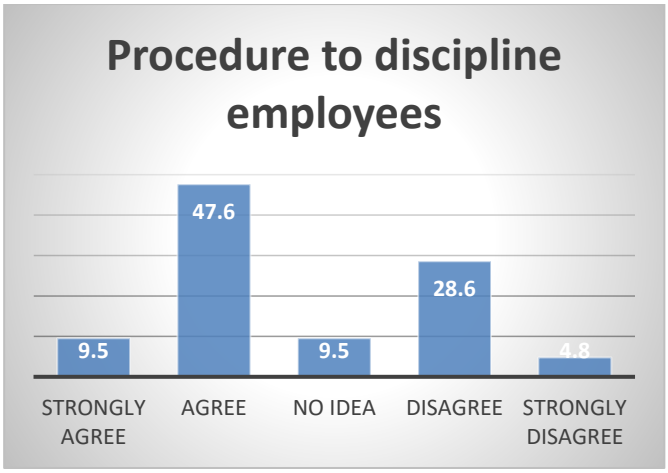


Figure 4.9 There is a Clear Procedure to Discipline Members who Violate Organisational Security Policy and Regulation.

Information-security policy enforcement was also considered as one of the important factors in creating a security culture according to the findings from the interviews. Figure 4.10 indicates that approximately 63 % of the respondents felt that security violations are reported. Enforcing security policy can be achieved by reporting and acting (Figure 4.11) against individuals who have been found to violate the organisation's security policy.

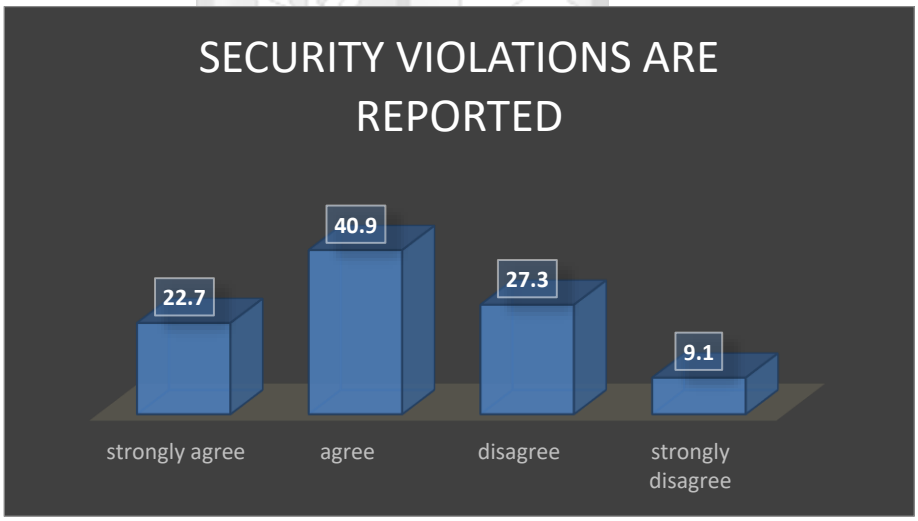


Figure 4.10 Information Security Violations are reported to the Proper Authority.

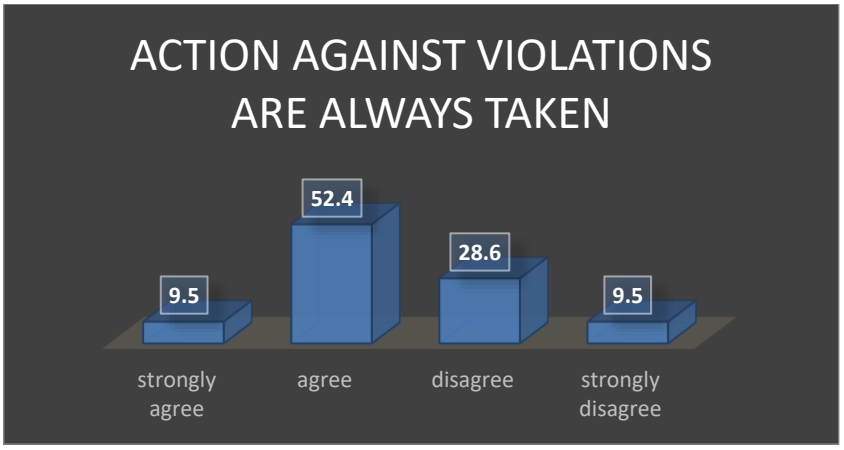


Figure 4.11 Action Against Security Violations is Always Taken.

It appears that lack of clearly defined policies and procedures contributed to lack of compliance at KNH. It seems the staff do not have considerable experience with managing security but largely depends on technical countermeasures (for example antiviruses and firewalls) in their quest to protect the hospital's information (Figure 4.5).

4.2.7 Information Security Training and Awareness

Kenyatta National Hospital adopts, among the various information security initiatives, trainning programs related to information security. This is undertaken by the IT department. Majority of the participants however indicated they do not receive adequate information security trainning,Figure 4.12.

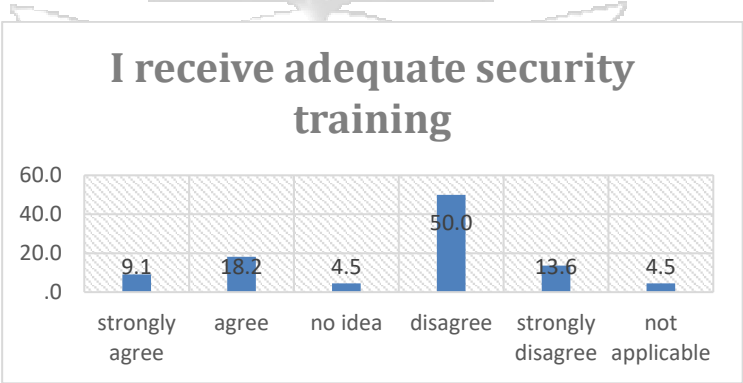


Figure 4.12 There is Adequate Information Security Training.

Management activities related to training programs are very crucial in achieving information security compliance to security policies and procedures.

4.2.8 Security Awareness

The case data revealed that there were no formal activities aimed at information security. A good number of participants indicated that they were not aware of their roles and responsibilities as far as information security is concerned.

Figure 4.13 Awareness of Information Security Roles and Responsibilities.

It seems awareness will play a pivotal role in the event of a security incident.

4.2.9 Information Security Commitment

Security ownership is a key part of security culture that was identified by the qualitative questionnaire findings.

Figure 4.14 and Figure 4.15 shows the respondents' perception on the construct of information security ownership. Overall, the users displayed strong security ownership. Most of the respondents felt that protecting the information of the organisation was an important part of their job.

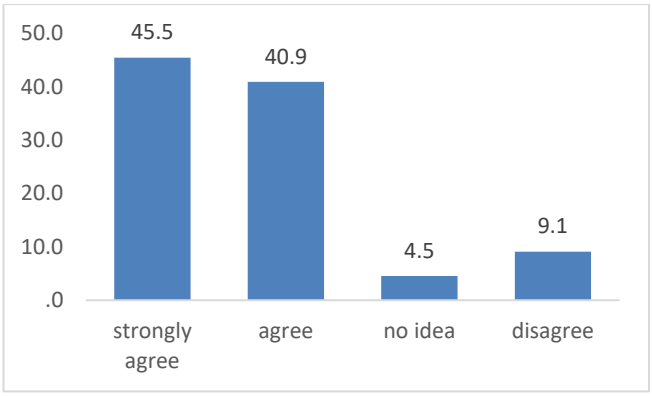


Figure 4.14 Ownership of the Outcomes of Information Security Decisions and Actions.

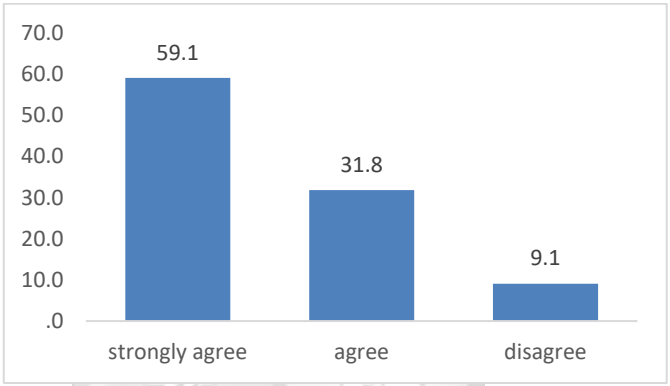


Figure 4.15 Responsibility to Protect Organisation's Information Assets.

Curiously, a small percentage of the respondents felt that they were averse to Information Security ownership. This is in conformity with the levels of awareness of roles and responsibility (Fig 4.13) and adherence to Information Security Policy (Fig 4.6 and Fig 4.7). The large number of respondents indicating that they take ownership of security decisions and actions is discordant with these outcomes. It is very difficult for staff to feel the ownership of protecting information when in the first instance they do not understand their roles and responsibilities. The ownership of Information Security will play a significant influence the behaviour of staff towards creation a mind-set of security culture. Further insights into this is revealed by the responses of participants as to what they think are the factors that influence security procedures. Figure 4.16 gives a summary of their responses.

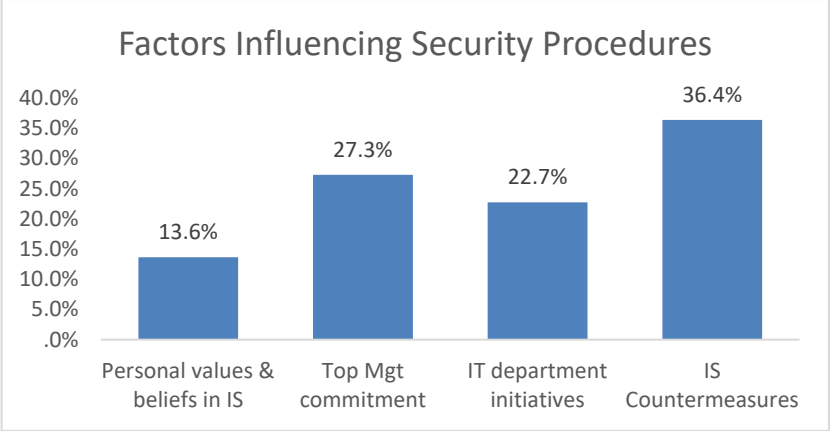


Figure 4.16 Factors Influencing Security Procedures

It can still be seen that only 13.6% of respondents felt that personal beliefs and values (culture) could influence Information Security.

4.3 Summary

This chapter detailed the analysis procedures and the assessment results for the information-security culture model to be developed in chapter 5. We identify the following as human factors cultivating Information Security Culture at Kenyatta National Hospital. These factors are:

- Top management support.
- Information Security Policy.
- Information Security Compliance.
- Information Security training and Awareness.
- Information Security Commitment.

Chapter 5 Proposed Framework

5.1 Introduction

From the interviews conducted and observations made, it is quite clear that the ENT clinic needs to have secure electronic medical records. Security measures need to be put in place that will match the complex and dynamic nature of the department. The medical records at the ENT clinic are currently accessed by any authorised personnel where the only security is a username and password. The patient files, which contain sensitive personal information, can also be found in the medical wards or at the examination rooms for outpatients.

A closer look at the outcomes of the literature review and analysis of the data gathered by the instruments, revealed that better information security could be achieved by addressing the following human factors at the clinic:

- Management Support
- Training and Awareness.
- Information Security Policy.
- Compliance.
- Sanctions and Rewards.

These aspects are driven by top management support since information security must also be aligned with the overall strategic goal of the organisation.

5.2 Management Support

The findings show that Management support is an essential driver of security culture creation. Management support could be instrumental in the improvement of security awareness by providing extensive training. It can also assist in enforcing and maintaining adherence to the security policy by the staff handling medical records. When management is committed to information security, they will ensure that appropriate individuals are responsible for specific information security activities for which they have been assigned. They will also ensure appropriate resource allocation, budget allocation and training of staff.

5.3 Security Policy

The outcomes also reveal that there is no clear Information security policy, this must be put in place as a priority. It is also necessary that mechanisms be put in place to ensure that these policies are enforced.

5.4 Security Compliance

Information security policies alone cannot protect the information of an organisation. Employees must comply with the security policies that have been put in place and management must lead by example to motivate the other employees. The degree of compliance by the employees is not encouraging.

5.5 Information Security Training and Awareness

Staff training is essential in raising awareness among employees and motivating them towards the correct security behaviour.

5.6 The proposed Framework

The proposed framework addresses the human factor and will therefore improve the security management of the medical records. The proposed framework is seen in Fig 5.1 below.

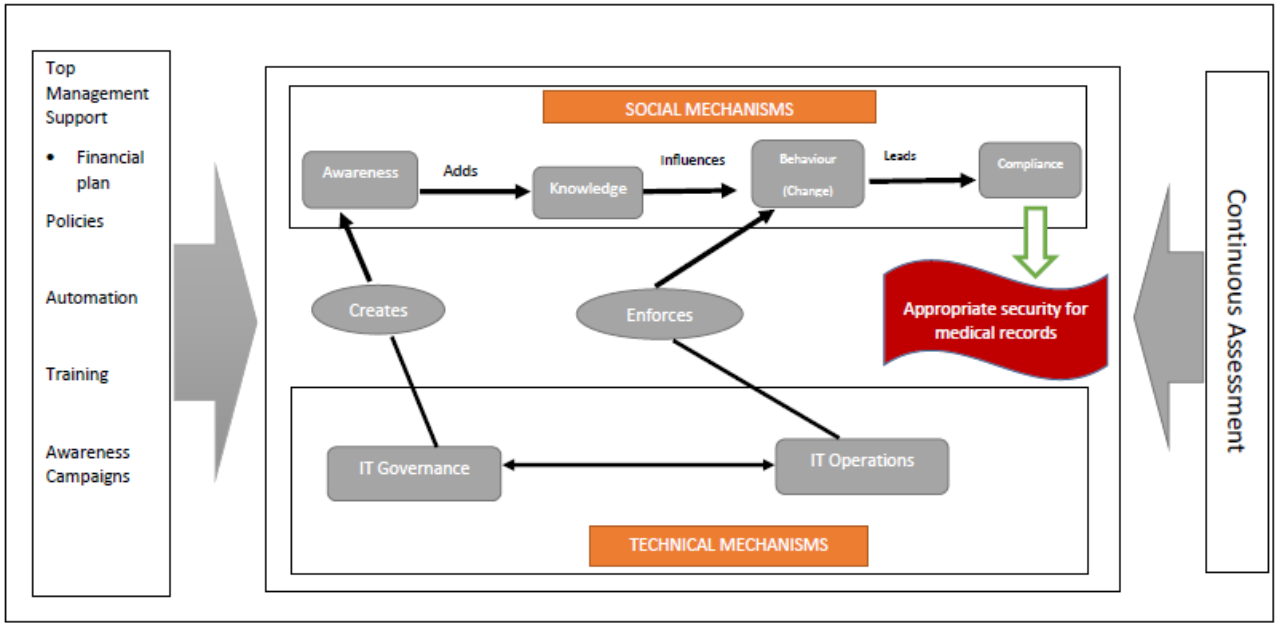


Figure 5.1 The New Beginnings Socio-Technical Framework.

The framework is divided into two zones, the technical mechanisms zone and the social mechanisms zone. These two zones are further divided into six distinct components. The various components are discussed in detail below.

a) IT Governance

IT Governance is an enabler of competitive advantage and to help achieve this, the framework makes use of the following drivers:

i) *Awareness campaigns* – all stakeholders need to have relevant information on a need-to-know basis in order to contribute to the operations of the organisation.

ii) *Policies* – these are strategic directives that form minimum standards, guidelines and day to day work instructions. They provide the standard procedures that form the working culture of the organisation. The goals of the security policy must be defined in conjunction with the security measures and practices that will be employed.

A clear procedure of reporting security related incidents must be put in place as this would significantly reduce any possibility of the even extending widely with cost to the organisation.

Ethical conduct policies must also be put in place by the organisation. These policies could assist users to understand and be aware of their security responsibilities.

iii) *Training* – these address the human capital that interact with and access the medical records. The institution must have a comprehensive approach to training and education, which includes quality standards, processes and skills for quality management of the medical records. In-service training should be instituted to educate and train employees. The training must be based on the security policy and guidelines must be set concerning their actions and attitudes.

iv) *Automatio*n – these are technological initiatives that will work towards eliminating human handling processes with aim of improving efficiency and effectiveness while reducing error.

v) *Accountability and Responsibility* – this involves creating a legal environment where actions are disclosed and are subject to scrutiny by the relevant departmental head in conjunction with the IT department.

b) IT Operations

IT operations will enable the provisioning of IT systems to run the records management processes. The IT department must provide customised and well-resourced solutions. This of course must be backed by a proper budget supported by top management. The technology measures used have role in shaping the information security culture of the organisation, and the information security culture shall support the effectiveness of different security technology measures.

c) Security Awareness

Security awareness is a fundamental pillar for creating a security culture. It is not reasonable to expect the existence a security culture if employees are not aware of the expectations regarding information security. Employees' lack of knowledge and awareness is considered a major threat to information security.

d) Knowledge

Increased knowledge will assist the employees of the organisation to understand the importance of a security culture. It will also lead to a better interaction with the systems of the organisation and result in acceptable procedures at any given time.

e) Behavioural Change

Knowledgeable employees and stakeholders are likely to demonstrate better behaviour during the interaction with the organisation's systems. A change in behaviour will contribute towards the protection of information of whatever kind. Information security will therefore become a natural aspect in the daily activities of the employees and stakeholders.

f) Compliance

Compliance will be achieved by enforcing security policies, reporting and taking action against individuals who violate the organisation's security policy. IT operations will additionally put in place technical measures that will ensure that policies are adhered to. However, enforcement will not be easy to accomplish if there is no strong support and

commitment from top management. This must therefore be an organisational priority to build a security culture.

h) Culture Assessment

This is crucial in making sure the emergent culture is in line with the vision of the top management.

5.7 Implementation of the Framework

5.7.1 Introduction

This section of the report presents the plan of implementing the proposed framework in the organisation with a view to improving the security of medical records and providing a directional structure for the management of records. The implementation stage involves management commitment, communication with all employees, education and training for all employees, and commitment by all employees. At this point, detailed activities, responsibilities, resources, schedules and a budget need to be defined (Schlienger and Teufel, 2005).

5.7.2 Guidelines for Implementation

The stakeholders in the implementation of the framework were as follows:

1) Top management
2) IT personnel
3) Health workers

The management was the key driver towards the implementation of the framework.

Table 5.1 gives implementation guidelines for the framework.

Table 5.1 Guidelines for Implementation of The Framework.

SRN	Component	Guideline
1	Stakeholders Forum	Brainstorming and identification of threat possibilities to the EHRs and establish priorities of all possible vulnerabilities

		Managers lobby for buy-in by all stakeholders, they show interest and commitment towards secure behaviour Put into perspective rewards and recognitions to individuals who contribute positively towards security measures.
2	IT Operations	IT management to give a current state of the infrastructure and ensure technical staff have the right training.
3	Training and Awareness	IT department trains workers on identities of possible threats and how to deal with them. Prepare material for training every morning and reduce the frequency as compliance has increased. Give historic examples of security breaches from other medical institutions as case examples
4	Continuous Assessment	Continually monitor safeguards and their effectiveness, share with workers and management as an when necessary. Carry out security audit by a reliable security firm to check the information system and also to encourage compliance due to fear of detecting non-compliant users.

5.7.3 The Outcomes of the Implementation

Table 5.2 shows a summary of the results of the implementation.

Table 5.2 Outcomes of the Implementation.

Component	Activities	Outcome
Management Support	• Assess the current state and identify gaps • Reach out for agreement across the entire department on how to implement an effective Governance, Risk & Management (GRC) program • Develop common processes for issue identification, issue management, remedial action and communication • Identify the starting point of the implementation • Train employees/users	• Updated and refreshed IT policies, procedures and controls circulated to employees • Communication channels with employees put in place. • Administrators listen to the workers whenever they report a problem, and this has encouraged the workers to be more open with reporting security issues. •
IT Operations	• Define an IT Strategic Plan • Identify Automated Solutions • Acquire and Maintain Application Software • Communicate Management Aims and Direction • Acquire and Maintain Technology Infrastructure • Sufficient power back up put in place • Security assessment survey	• Technical controls implemented • System is running even when power is lost from the national grid. • Specific responsibilities allocated • Employees actions with the **IS** more visible • IT technical support are mandated to be available if and when needed.
Skills and Training	• Develop and/or purchase training material. • Implement tracking mechanism to trace who completes training and	• Regular email communication is used to remind staff

	when Dummy system implemented. • System administrators are well trained. • Personnel in charge of various units are well trained.	of the importance of security policies. • Unit heads monitor the people reporting to them and ensure and ensure that their behaviour is secure. • Every morning employees use the dummy system to role play a security scenario. • Employees improving in their use of security functions within different applications
Awareness and Knowledge	• Assess current state and identify gaps. • Set up a security awareness team. • Determine roles for security awareness. • Train employees and users • Checking how often users change their passwords	• All personnel: ▪ recognise threats ▪ report potential security issues • Passwords changed regularly and system administrators monitor these and address deviant behaviour.
Behavioural Change	• Assess lost productivity. • Assess how employees/users interact with system	• Better adherence to security requirements by employees • All work files locked up at the end of each day.
Compliance	• Identify, classify and protect information. • Monitor information security practices and procedures to ensure compliance with policy	• Plans to reward &recognise those who do the right thing for security are being discussed. • Employees demonstrating ownership of need to protect information.

		• Security violations are being handled on merit
IT Governance	• Deploy IT governance tools. • Embed IT governance within the organisation	• Short, medium and long-term strategies set. • Standard procedures being put in place. • Training plans set up
Continuous Assessment	• Put in place cycle for reviewing performance of outcomes. • Develop key performance indicators	• Management strategic planning reviews strategy from time to time.

5.8 Framework Validation

Validation is defined as "the process of ensuring that the model is sufficiently accurate for the purpose at hand" (Carson, 1986).

To validate this framework, a survey was conducted to establish a consensus among the people who interact with medical records at the ENT clinic. These same people had previously been interviewed before the implementation of the framework to establish the state of information security culture within the clinic. The aim of the survey was to validate the task of each component and the component to information security culture. The survey questionnaire used in the survey is available in **Appendix D.**

Thirty-five participants were invited to the online survey to review the components of the proposed framework in relation to the outcomes of its implementation. Twenty-five of them took the online survey and submitted their responses. Their feedback was collected and analysed using SPSS to validate each component of the proposed framework. Each component was translated into several statements that represented the component. A ranking scale was used to evaluate and indicate the level of importance of each task (Table 5.2). A score of 0 – 5 was used to rate the response with zero meaning not applicable to five meaning highly important.

Table 5.3 Survey Scale.

N/A	Very Low	Low	Average	High	Very High
0	1	2	3	4	5

Figure 5.2 shows an extract from the survey.

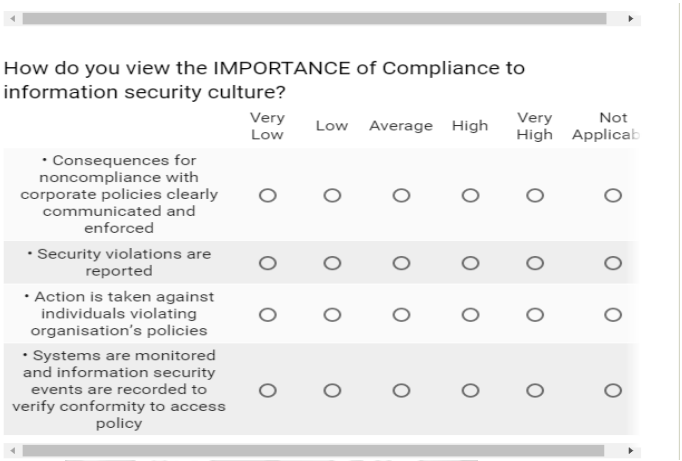


Figure 5.2 Extract from the Survey.

5.8.1 Results

After the responses were collected and combined, the results were analysed to validate the framework.

For a model to be valid and practical, it must be reliable (AlHogalil, 2015). Cronbach's alpha, a coefficient of internal consistency, was used to measure reliability, providing an indication of how consistent the responses were across items within the scale.

Cronbach's alpha values must meet the minimum accepted criteria (above 0.7) to confirm the consistency and reliability of the framework (Da Veiga et al., 2007). The results of the reliability analysis are presented in Table 5.2 and Table 5.3.

Reliability Analysis

A summary of the reliability analysis of the whole framework is presented in Table 5.3

Table 5.4 Summary of Reliability Analysis.

Cronbach's Alpha	Number of Items
.954	23

The Cronbach's alpha is 0.954, which indicates a level of internal consistency for the scale used.

The reliability analysis for the different components of the framework are presented in Table 5.4.

Table 5.5 Reliability of Components of The Framework.

Component	Number of Items	α value
IT Governance	3	.881
IT Operations	4	.813
Security Awareness	2	.886
Knowledge	2	.871
Behaviour Change	4	.847
Compliance	4	.835
Top Management Commitment	4	.919

All the values of the Cronbach's alpha are above 0.8, which is larger than the threshold. This indicates a good internal consistency and reliability. This implies that the instrument is composed of a set of consistent variables for capturing the meaning of the components of the framework.

Framework Validation Discussion

Preliminary findings before the framework was implemented indicated that there were major concerns in the information security environment at the ENT clinic. Among the top three causes of security threats was non-compliance. Many of them felt that non-

compliance was a result of inadequate technology and little or nothing to do with personal values and beliefs. There was also lack of skills and training. Other findings included:

- Lack of proper procedures and roles.
- Involvement of senior leadership
- Lack of clearly defined information security policies

It has shown that the seven basic dimensions have been accepted. This indicates that the structure of the proposed framework is valid and is approved. It can be concluded that the information security culture that affects user security behaviour will be the result of interaction between the social and technical aspects. This emphasises that security is not purely a technical issue but must involve the employees as well.

A comprehensive framework is important to ensure all the factors pertaining to information security are covered.

5.9 Summary

This chapter provides a discussion of the findings of this study as they relate to the research questions presented in Chapter 1. An Information Security framework is proposed to assist firms in implementing information security components in such a manner that they would positively direct employee behaviour towards the protection of information assets.

A model to enhance information security culture that promotes acceptable information security behaviour was designed and validated through expert review.

The research findings showed that information security of medical records is greatly influenced by behavioural intentions of employees. The framework presented here is credible as seen from the validation by experts. The implementation process has also revealed a significant change in the behaviour of users towards information security. The ENT department has begun to realise a better security culture amongst its employees.

Chapter 6 Discussion

6.1 Introduction

Kenyatta National Hospital is the largest referral hospital in Kenya and will therefore have a lot of medical data of patients. As of November 2012, KNH had four million digitised records (Kenyatta National Hospital, 2012). This medical data contains a lot of sensitive information apart from the clinical information that is collected and recorded by the staff working with patients in the hospital. It is therefore imperative that a management framework that improves the security of this information be put in place.

6.2 Discussions and Implications

This study investigated the human factors and their impact on information security culture. In this attempt we addressed the following objectives.

1. Examine the human factors that currently constitute or reflect information security culture.
2. Examine the state of information security culture at Kenyatta National Hospital.
3. Design a framework that would ensure better security management of Electronic Medical Records.
4. Validate the information security framework.

The picture that emerges from the above analysis of the data is that human factors can be used to cultivate a strong information security culture. Establishing a security subculture within an organisation will facilitate the dissemination of information security principles (Da Veiga and Martins, 2015).

The results of this study indicated that 56.7% of the respondents believe that human beings are a source of threat to information security. These findings are consistent with several of studies (Acuña, 2016; Öğütçü, et al., 2016; van Niekerk, 2010). The other 43.3% believe that security threats are only a result of technology related issues like viruses and hardware failure. This implies that a significant number of users do not consider themselves as a possible threat to information security. This is concerning as it indicates lack of security awareness among the employees.

73% of the participants agreed that management support is important in a security program. They felt that the management was involved in the security procedures at the department. Several studies (Aurigemma and Mattson, 2017; Corris, 2010; da Veiga and Martins, 2015; Fagerström, 2013; Glaspie, 2018; van Niekerk, 2010) support this sentiment. However, this observation cannot be considered in isolation since management involvement cuts across many aspects of the organisation and indeed other facets of information security. Further consideration of the findings show that 50% of the participants reported that there were no clear policies on security, 33% indicated that there were no clear sanctions/deterrent measures against violations of security, 36% reported that security violations are not reported and if they are reported then 38% said no action is taken against the offenders. It seems possible that the management have the knowledge and the will but no push to implement.

Further to this, 67.7% of the employees reported that they have no adequate training on information security, 48% are not aware of their security responsibilities and more that 30% said they do not comply with security policies. Many studies (Da Veiga, 2015; Tarimo, 2006; von Solms, 2004; Whittman and Mattord, 2011) have identified staff training and awareness as important in the establishment of a security subculture. Employees who are aware of security requirement are likely to comply with those requirements (van Niekerk, 2010; von Solms, 2004).

The results of this study did not show the presence of any strong security culture in Kenyan medical institutions. Only 13.6% of respondents at KNH felt that personal beliefs and values could influence Information Security. When asked the question:

"Do you think personal values and beliefs influence security related behaviours?"

One of the respondents said:

"Despite clear policy regarding information (security), human behaviour is inclined to falsification of documentation for self-benefit."

Another one responded thus: *"Yes. The beliefs are the old ones of the bosses (top management) not wanting change."*

Yet one more responded as follows:

"Yes. You cannot release any information pertaining to individual staff un-procedurally"

One respondent had a very different perspective and responded as follows:

"No. Security related behaviours is part of policy and practice and therefore personal values and beliefs have nothing to do with it."

Whichever way we look at these responses, they point to the fact that personal values and beliefs, in other words ***culture***, plays an important role in Information Security.

A report by (Okuttah, 2012) indicated that Kenyatta National Hospital would spend 20 million Kenya shilling to digitise some of the medical records. This is consistent with an observation (Herath and Rao, 2009) that organisations are spending substantial amounts of money on technologies. However, good security cannot be bought through software and hardware (Tessem and Skaaraas, 2005). Effective information security depends on three components, namely: people, processes and technology (Herath and Rao, 2009). This study found the people component wanting in KNH and therefore proposed a management framework that addressed this component. The framework was implemented and validated.

A deliberate management support is necessary to make the creation of this culture a success. Humans have the innate ability to do good and this ability can be trained to become the strength of information security in an organisation. This is evident from the result that 80% of the employees accept that it is their responsibility to protect the information of the organisation. Using the recommended framework, the management at the ENT clinic was able to begin the steps towards creating a security-aware culture.

Studies (Hannan et al., 2000; Kanyua, 2015; Lelei, 2010; Makumbi et al., 2012; Odiwuor et al., 2015) indicated that employees in Kenyan medical institutions need training and awareness on information security. In addition to this, Lelei (2010) reported that up to 60% of doctors, clinical officers and laboratory technicians have shared their passwords. These findings paint a grey picture about the state of information security culture in medical institutions in Kenya. We therefore recommend this framework to be implemented by other

hospitals in Kenya. An information security culture will be helpful in improving the security of medical records.

6.3 Benefits of Implementing the Framework

From the research findings highlighted in Chapter 4, and the outcomes of the implementation of the framework, the following is a list of how the health workers will use the framework to improve the security of the EMRs.

- Information security policies are clearly defined and available to the health workers.
- Management now budgets for training of health workers. They take the initiative to offer on-going training to the workers to know what to do, how to do it and why they do it. The health workers are now more aware of sources of security threats and take precautions so that they are not that weakest link in the organisation.
- The management meets regularly with the health workers to motivate them to accept the security measures. This is going on well since majority of the employees had already indicated their willingness and commitment to protect the information. The management has decided to listen more to the health workers instead of using threats and sanctions. This has worked well for them since workers feel free to report their errors and seek for guidance.
- Level of compliance, which was previously low, is now higher. Employees are now aware of the policies and do everything to ensure they comply with the policies. The risks of security incidents are now reduced.
- The management is planning to have regular security audits. This will assist them in reducing risks, strengthen controls and continually monitor information security alignment with strategic goals of KNH.
- Deterrent measures are being discussed so that clear guidelines on these can be put in place

6.4 Conclusion

From the findings of the study it would be safe to assume that information security issues must now shift from the IT department to the management. Teaching people and encouraging them to report any problem is working better than employing deterrent

measures. Workers feel like they belong and have a better security behaviour, freely reporting any possible security threat or breach and this gives the technical staff and easier way to hand such issues. This would be instrumental in aligning information security goals with the strategic goals of the organisation and to move away from a security based on technology to one that is cognisant of the human factor behind the technology.

Chapter 7 Conclusions and Recommendations

7.1 Conclusions

The Electronic Medical records at KNH are not secure. The human factor is a major threat to these records and must therefore be handled in the best way possible to improve the security of the records. Access restrictions to storage of the records and employees having usernames and passwords is not a sufficient condition for their security. With sufficient motivation, the employees can share information regarding the patient with an outsider and no one will know that this happened. This will result in the loss of privacy to the patient or some daring criminally minded individuals may use that leaked information for financial gain.

The employees have no adequate training on matters regarding information security even though the Top Management seems to be aware of security needs. This boils down to the lack of management support as evident from the study. Security policies are not well defined or clearly stated and understood by the employees and stakeholders handling the medical records. As a result, employees are not aware of their roles and expectations in as far as Information Security is concerned. A significant number of them are apathetic to the security behaviour of their colleagues. They would therefore not even report any security incident concerning them.

The implementation of the proposed framework will aid the organisation in improving the security of the medical records since it addresses the human factor and links this with technical aspects that would be helpful in enforcing compliance to the policies that would be put in place. Cultivating a security culture within the organisation enhances ownership and hence the "this-is-how-we-do-it-here" attitude within employees will become better. The employees have demonstrated commitment towards ensuring the security of the information. What is now needed is for the management to take advantage of this and continue with the training and awareness programs.

7.2 Recommendations

i. The current study provides a reliable and valid information security framework that can be used by any hospital that has or intends to have electronic medical records.

ii. Information security managers can use the outcomes of this study to implement effective information security management approaches.
iii. The current study can be used as a reference point for other studies on information security culture. This may be in a different context or environment.

7.3 Future Work

The research work reported here was set out to examine the state of information security in medical institutions in Kenya. Given that very little information was found in this respect and from the findings presented in chapter 4, the next stage of research can undertake the following aspects:

i. Culture is organic and may vary from one community or location to another. We therefore recommend that further work be done nationwide to get a national view of information security culture in the different public hospitals.
ii. During the advanced studies, questionnaires and interview respondents may include patients and other stakeholders as well.

References

Acuña, Dennis C., "Effects of a Comprehensive Computer Security Policy on Computer Security Culture" (2016). MWAIS 2016 Proceedings. 10. http://aisel.aisnet.org/mwais2016/10

Ahlan, A. R., Lubis, M., Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. Retrieved on 6/29/2020 from: https://www.sciencedirect.com/science/article/pii/S1877050915036121

Alavi, R. (2016). A Risk-Driven Investment Model for Analysing Human Factors in Information Security. Retrieved on 6/28/2020 from: https://repository.uel.ac.uk/download/353398f1bcb3a71a836df15af8c0e2d69285f43abb0e8a174775b5fe42d2267e/2026040/Thesis%20FINALpdf.pdf

Alhogail, A. (2015). Design and Validation of Information Security Culture Framework, Computers in Human Behavior, vol. 49, no. August, pp. 567–575, 2015.

Alnatheer, M. & Nelson, K. (2009). *A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context*. Retrieved on 11/05/2015 from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=ism

Alnatheer, M. A. (2012). Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia. Retrieved 01/12/2015 from: http://eprints.qut.edu.au/64070/1/Mohammed_Al_Natheer_Thesis.pdf

Aurigemma, S. and Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Retrieved on 6/28/2020 from: https://facultystaff.richmond.edu/~tmattson/Status_Computers_Security_2017.pdf

Appari, A. and Johnson, M. E. (2010) 'Information security and privacy in healthcare: current state of research', *Int. J. Internet and Enterprise Management*, Vol. 6, No. 4, pp.279–314. Retrieved on 25/5/2012 from: http://www.ists.dartmouth.edu/library/501.pdf

Wycliffe Nyabayo Ayieko (2016). Physicians Use of Electronic Health Records Systems and Performance in Hospitals Within Nairobi County, Kenya. Retrieved on 6/23/2020 from: http://erepository.uonbi.ac.ke/handle/11295/99447

Benoot, C., Hannes, K. & Bilsen, J. The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Med Res Methodol* **16,** 21 (2016). https://doi.org/10.1186/s12874-016-0114-6

Box, D. and Pottas, D. (2014). Improving information security behaviour in the healthcare context. Retrieved on 6/18/2020 from: https://reader.elsevier.com/reader/sd/pii/S2212017313002764?token=396717934860F384E5C370BE39B6373F3572A9BB00D15FC3CAA55683A29AF8545ED85E1E95452984D265F158FED3354B

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Retrieved on 6/27/2020 from: http://130.18.86.27/faculty/warkentin/BIS9613papers/MISQ_SpecialIssue/BulgurcuCavusogluBenbasat2010_MISQ34_RationalityAwareness.pdf

Carson, J.S., 1986. Convincing Users of Model's validity is Challenging Aspect of Modeller's Job. Industrial Engineering. 18 (6): p. 74-85.

Corriss, L. (2010). Information Security Governance: Integrating Security Into the Organizational Culture Position Paper. Retrieved on 6/25/2020 from: https://dl.acm.org/doi/pdf/10.1145/1920320.1920326

Creswell, J. W. (2008). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (3rd ed.). New Jersey: Pearson Education.

D'Arcy, J., and Greene, G. (2009). The Multifaceted Nature of Security Culture and Its Influence on End User Behavior. Paper presented at the IFIP TC 8 International Workshop on Information Systems Security Research, Cape Town, South Africa.

D'Arcy, J. and Devaraj, S. (2012). Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. Retrieved on 6/29/2020 from: https://onlinelibrary.wiley.com/doi/full/10.1111/j.1540-5915.2012.00383.x

Da Veiga, A. and Eloff, J. H. P. (2007). An Information Security Governance Framework. Retrieved on 3/5/2015 from: http://uir.unisa.ac.za/bitstream/handle/10500/14338/An%20Information%20Security%20Governance%20Framework.pdf?sequence=1&isAllowed=y

Da Veiga, A., Martins, N. and Eloff, J.H.P. (2007). *Information security culture – validation of an assessment instrument*. Retrieved 3/5/2015from: http://uir.unisa.ac.za/bitstream/handle/10500/13582/Information%20security%20culture.pdf

Da Veiga, A. and Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study, *Computers & Security*, Volume 49, March 2015, Pages 162-176, http://dx.doi.org/10.1016/j.cose.2014.12.006

Fagerström, A. (2013). Creating, Maintaining and Managing an Information Security Culture. Retrieved 13/05/2015 from: https://publications.theseus.fi/bitstream/handle/10024/63254/Fagerstrom_Alex.pdf?sequence=1

Fulford, H. and Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. Retrieved on 16/01/2015 from: https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/8233/1/%20Uptake%20%5BIM%20%26%20CS%5DUptake%20of%20ISP%20_IM%20%26%20CS%20-%20Repository%20Copy_.pdf

Gebrasilase and Lessa. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. Retrieved on 08/05/2015 from: http://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1019&context=ajis

Glaspie, H. (2018) Assessment of Information Security Culture in Higher Education. Retrieved on 6/21/2020 from: https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=7009&context=etd

Hadjor, G. T. and Gadasu, E. K. (2014). The Influence of Organizational Culture on Information Security Policy Success. Retrieved on 7/2/2020 from: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1025968&dswid=-954

Han, J., Kim, Y.J., Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*. 66. 52-65.

Herath, T. and Rao, H. R. (2009). Encouraging Information Security Behaviors In Organizations: Role Of Penalties, Pressures And Perceived Effectiveness. Retrieved on 08/05/2015 from: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/HerathRao2009_DSS_PenalitesPressures.pdf

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? Retrieved on 6/29/2020 from: https://dl.acm.org/doi/pdf/10.1145/1953122.1953142 6/29/2020

Ifinedo, P. (2013). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition, Information & Management (2013), http://dx.doi.org/10.1016/j.im.2013.10.001

Macharia Kamau (2012, October 15). Kenyatta National Hospital digitisation almost complete. The Standard. Retrieved on 6/23/2020 from: https://www.standardmedia.co.ke/article/2000068438/kenyatta-national-hospital-digitisation-almost-complete

Manetje and Martins. (2009), The relationship between organisational culture and organisational commitment Southern African Business Review Volume 13 Number 1 2009

Martins, A. &Eloff, J.H.P. (2002). Information security culture. Retrieved on 28/03/2015 from: https://ujdigispace.uj.ac.za/handle/10210/292

Mikko Siponen, Seppo Pahnila, and Adam Mahmood (2007). Employees' Adherence to Information Security Policies: An Empirical Study. Accessed on 07/03/2015 from: http://opendl.ifip-tc6.org/db/conf/sec/sec2007/SiponenPM07.pdf

Myyry,L, Siponen, M., Pahnila, S., Vartiainen, T and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Retrieved on 7/7/2020 from: http://130.18.86.27/faculty/warkentin/BIS9613papers/EJIS_SpecialIssue/Myyryetal2009_EJIS_18_2_policycompliance.pdf

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Essex, England: Pearson.

NIST. (2006). I n f o r m a t i o n S e c u r i t y. Retrieved on 07/03/2015 from: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Okubasu, B. (2020, March 18). Health Data is Sensitive. *Daily Nation.* Retrieved on 6/21/2020 from: https://www.nation.co.ke/kenya/healthy-nation/we-need-to-protect-health-data-avoid-breach-256498

Okuttah, M. (2012, June 7). Kenyatta Hospital starts digitising 40m records to cut costs. Business Daily. Retrieved on 7/9/2020 from: https://www.businessdailyafrica.com/corporate/539550-1423034-12mp1as/index.html

Pable, J. (n.d.) Research on the homeless population: the particular utility of case study methodology Retrieved on 6/29/2020 from: https://www.academia.edu/2664894/Research_on_the_homeless_population_the_particular_utility_of_case_study_methodology

Pallant, J. (2010). SPSS survival manual: A step by step guide to data analysis using SPSS for windows. Berkshire, England: Open University Press.

PwC. (2015). 2015 Information Security Breaches Survey. Retrieved on 6/26/2020 from: http://www.pwc.co.uk/assets/pdf/2015-isbstechnical-report-blue-03.pdf

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Safa, N. S., Von Solms, R., Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 1-13.

Salahuddin-Alfawaz (2011). Information Security Management: A case study of an information security culture. Retrieved on 15/05/2014 from http://eprints.qut.edu.au/

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Retrieved on from http://saim.pub.ro/biometric/Alte_articole/Assessing%20insider%20threats%20to%20information%20security.pdf

Schlienger, T. and Teufel, S. (2005). Tool supported management of information security culture. Retrieved from http://opendl.ifip-tc6.org/db/conf/sec/sec2005/SchliengerT05.pdf

Stake, R. E. (1994). *Case studies.* In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (p. 236–247). Sage Publications, Inc.

Tarimo, C. N. (2006). ICT Security Readiness Checklist for Developing Countries: A social-Technical Approach. Retrieved on 05/08/2015 from: http://su.diva-portal.org/smash/get/diva2:189935/FULLTEXT01

Van Niekerk, J. F. (2010). Fostering Information Security Culture Through Integrating Theory and Technology Retrieved on 6/27/2020 from: https://pdfs.semanticscholar.org/be30/7fe1c35e58da0340ea22d72676b3c914c1a9.pdf

Van Niekerk, J. and Von Solms, R. (2006). Understanding information security culture: a conceptual framework. In proceedings Information Security South Africa (ISSA), Johannesburg, South Africa. Retrieved on 07/03/2016 from: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Van Niekerk, J.F. and Von Solms, R. (2010). Information security culture: A management perspective. Retrieved on 07/03/2016 from https://www.researchgate.net/profile/Johan_Van_Niekerk2/publication/223848732_Information_security_culture_A_management_perspective/links/53e75b790cf21cc29fd9cf44.pdf

Von Solms R. and Von Solms, B. (2004). From policies to culture. Retrieved 07/03/2016 from http://84.205.229.18/securityc/d/english/Culture/From%20policies%20to%20culture.pdf

Yin, R. K. (2003) Application of Case Study Research, Second edition, California: Sage Publications Inc.

Appendix A: Letter to Participants

LETTER TO PARTICIPANTS

Dear

I am carrying out a research at Strathmore University, focusing on potential solutions to management of Information security of medical records.

As part of the research, your organisation has been chosen to participate as a case study.

In particular, staff dealing with or handling medical records.

Information presented by interviewees will only be used for purposes of this research. In the description of the results of this survey, no identification of individual persons will be made. Individual answers will be kept confidential, that is the answers will be analysed and presented by category of staff and the organisation.

Thank you in advance for your valuable time and consideration.

Sincerely,

Theodulus O. Otieno

Strathmore University

Nairobi

Email: otieno.odhiambo@gmail.com

Appendix B: Questionnaire

** NO NAME IS REQUIRED IN THIS QUESTIONNAIRE

EMPLOYEE:

RECORDS ☐

NON-RECORDS ☐

NON-EMPLOYEE ☐

DESIGNATION:

DATA CLERK ☐

DOCTOR ☐

RESEACHER ☐

OTHER (Specify)

…….

DEPARTMENT:

Medical records ☐

Emergency ☐

Nursing ☐

Other (Specify)

……

LEVEL OF EDUCATION:

Primary ☐

Secondary ☐

Post-Secondary ☐

University ☐

Post Graduate ☐

1 What do you consider to be the top three main possible causes of security incidents in your organisation?

- ☐ Viruses and malicious software
- ☐ Cyber or internal based attacks
- ☐ User error or non-compliance
- ☐ Hardware failure
- ☐ System administrators' error or non-compliance
- ☐ Other (please specify)

2 In your view, what do consider to be the top three barriers to improved or better security compliance in your organisation?

- Lack of adequate technology
- Clear direction in security procedures and roles
- Lack of awareness and training programs
- Other (please specify)

3 How do you think the following will influence security procedures in your organisation? Please rank.

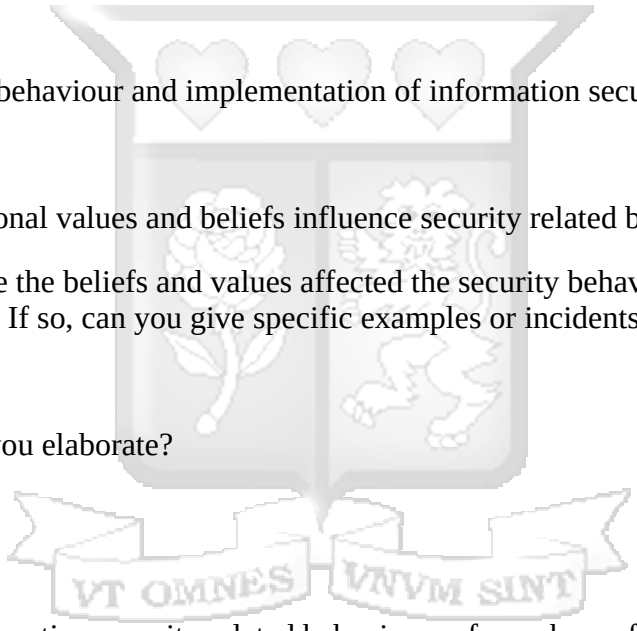
- Personal values and beliefs on information security
- Top management commitment (e.g. strong support including allocating sufficient budget)
- IT department initiatives (e.g. policies, training, sanctions, guidelines)
- Information security countermeasures (e.g. antiviruses, firewalls)

Part 2: user behaviour and implementation of information security management

1 do you think personal values and beliefs influence security related behaviours?

If YES, have the beliefs and values affected the security behaviours of you colleagues at work? If so, can you give specific examples or incidents?

If NO, can you elaborate?



2 do you think information security related behaviours of members of your organisation can be influenced by managerial security initiatives like policies, guidelines and training programs?

If YES, how is it likely to affect staff adherence to information security policy

If NO, what makes you think so?

3 Do you believe information management standards could serve a useful purpose in managing your organisation's information security effectively?

If YES, how?

If NO, why?

4 Do you believe a long term strategy on information security is important in addressing matters related to information security?

If YES, how?

If NO, why?

5 What other specific information security related issues and factors are you likely to encounter in terms of the effectiveness of the information system if implemented in your organisation?

6. Please choose the answer that best describes your opinion about your organisation.

Statement	**Strongly Agree**	**Agree**	**No idea**	**Disagree**	**Strongly Disagree**	**Not Applicable**
Top management considers information security an important organisational priority.						
Senior management						

gives strong and consistent support to the security program.						
Senior management is always involved in key information security activities.						
Management ensures that appropriate individuals are made responsible for specific information security aspects.						
Management ensures that everyone who takes information security actions, and makes information security decisions is held accountable for their decisions and actions.						
Information security violations are reported to the proper authority.						
Actions against violations are always taken.						

There is a clear procedure to discipline members who violate organisational security policy and regulations						
Information security policy is clearly defined.						
I receive adequate information security training.						
I am aware of my information security roles and responsibilities.						
I always adhere to the information security policy.						
Others around me adhere to information security policy						
It is my responsibility to protect the information of my organisation						
I take ownership of the outcomes of my information security decisions and actions						

Appendix C: Interview Guide

1 Do you think personal values and beliefs influence security related behaviours?

If YES, have the beliefs and values affected the security behaviours of you colleagues at work? If so, can you give specific examples or incidents?

If NO, can you elaborate?

2 Do you think information security related behaviours of members of your organisation can be influenced by managerial security initiatives like policies, guidelines and training programs?

If YES, how is it likely to affect staff adherence to information security policy

If NO, what makes you think so?

3 Do you believe information management standards could serve a useful purpose in managing your organisation's information security effectively?

If YES, how?

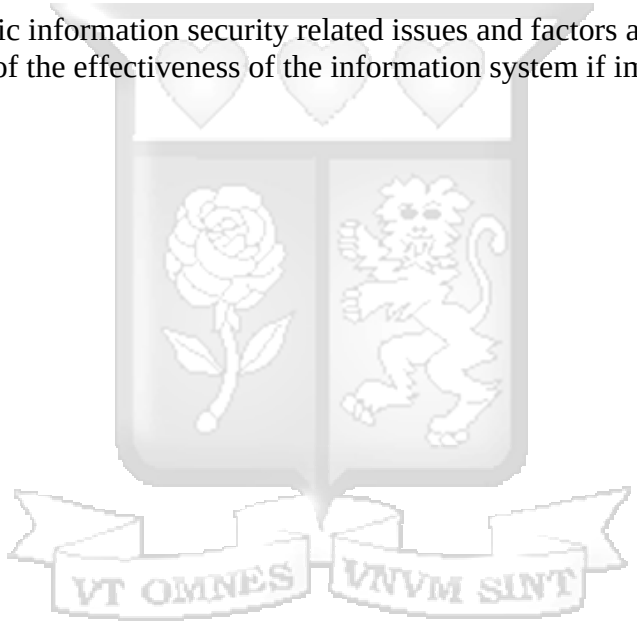
If NO, why?

4 Do you believe a long term strategy on information security is important in addressing matters related to information security?

If YES, how?

If NO, why?

5 What other specific information security related issues and factors are you likely to encounter in terms of the effectiveness of the information system if implemented in your organisation?



Appendix D: Information Security Culture Survey

Information Security Culture Survey

Research indicates that humans are responsible for 80% of security breaches to information. In this research, we are looking at ways to address the human factor. This form seeks your expert opinion regarding the proposed New Beginnings Security framework. This framework has been proposed to help mitigate the security of Electronic Medical Records. Each question has several answer options which you need to consider. This will take just a few minutes of your valuable time.

The Proposed framework

Components of the framework

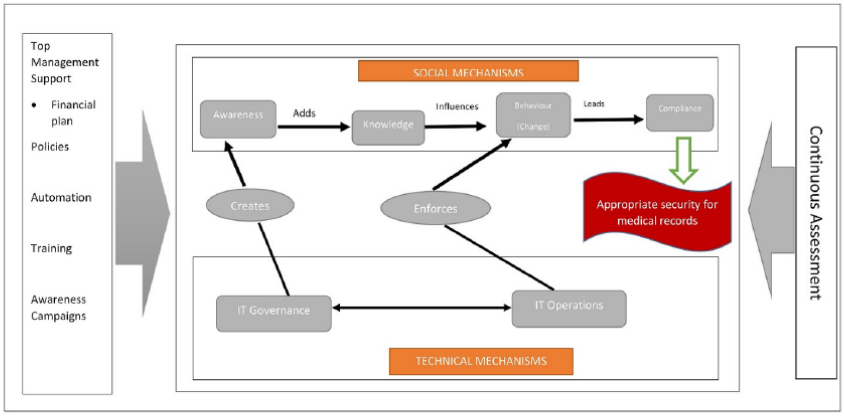


Fig 5.2 The New Beginnings Socio-Technical framework

How do you view the IMPORTANCE of IT Governance to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• IT Strategy is well defined	○	○	○	○	○	○
• Management aims and direction are communicated well to employees	○	○	○	○	○	○
• Role base structures are clearly defined	○	○	○	○	○	○

How do you view the IMPORTANCE of IT Operations to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• Assess and manage IT risks and dangers around the environment	○	○	○	○	○	○
• Acquire and maintain application software	○	○	○	○	○	○
• Acquire and maintain technology infrastructure	○	○	○	○	○	○
• Enable operation and use of the IT system	○	○	○	○	○	○
• Systems are monitored and information security events are recorded to verify conformity to access policy	○	○	○	○	○	○

How do you view the IMPORTANCE of Security awareness to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• Expectations regarding information security is spelt to employees	○	○	○	○	○	○
• All users are made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of organisational assets.	○	○	○	○	○	○

How do you view the IMPORTANCE of Knowledge to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• Employees understand the importance of security culture	○	○	○	○	○	○
• Employees interact better with the information system of the organisation	○	○	○	○	○	○

How do you view the IMPORTANCE of Behaviour change to information security culture?

	Very Low	Low	Average	High	Very High	Not applica
• Employees are more likely to report behaviours/activities of concern	○	○	○	○	○	○
• Employees demonstrate ownership of the need to protect information security	○	○	○	○	○	○
• Employees understand the security risks associated with their actions	○	○	○	○	○	○
• Assesses the perceptions about change and the willingness of users to change in order to protect information	○	○	○	○	○	○

How do you view the IMPORTANCE of Compliance to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• Consequences for noncompliance with corporate policies clearly communicated and enforced	○	○	○	○	○	○
• Security violations are reported	○	○	○	○	○	○
• Action is taken against individuals violating organisation's policies	○	○	○	○	○	○
• Systems are monitored and information security events are recorded to verify conformity to access policy	○	○	○	○	○	○

How do you view the IMPORTANCE of Top management commitment to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• Information security function has the authority it needs to manage and ensure compliance with the information security program	○	○	○	○	○	○
• Information security function has the resources it needs to manage and ensure compliance with the information security program	○	○	○	○	○	○
• Written information security policies are consistent, easy to understand, and readily available to administrators, faculty, employees, students, contractors, and partners	○	○	○	○	○	○
• Responsibilities are in place to ensure employees', contractors', or third party users' exit from the organisation is well managed	○	○	○	○	○	○

How do you view the IMPORTANCE of Culture assessment to information security culture?

	Very Low	Low	Average	High	Very High	Not Applica
• Strategy is reviewed and updated at least annually or more frequently when significant changes require it	○	○	○	○	○	○
• It is crucial to understand the perceptions, attitudes and behaviour of the organisation's employees	○	○	○	○	○	○

Appendix E: Main Security Threats in Kenya

Type of organisation	Main threats	Countermeasures	
		Strengths	**Weaknesses**
Small financial services	Viruses; Theft of IT resources, destruction of IT resources; **unauthorised access by employees;** financial fraud; misuse of the internet by employees especially by spending time on social sites	Availability of Security Policy; Firewall; usernames and passwords; offsite and local backups; antivirus	**Lack of awareness** on security policy; Security policy not enforced; negligible IS security budget; no dedicated security personnel
Investment Bank 1	Hackers; competitors; **disgruntled employees;** users in general; viruses; lack of knowledge on security issues	Firewalls; Antivirus software is kept up to date; security policies and procedures;	Lack of dedicated security personnel
Investment Bank 2	Hackers; competitors; **disgruntled employees;** users in general; viruses; partners and suppliers with access to IT resources; **External IT contractors with access to systems**	Firewalls; encryption; risk assessments; database of incidents and their resolution;	Lack of dedicated security personnel
Commercial Bank 1	Viruses; hackers; **disgruntled employees;** system users; suppliers or partners with access to their systems;	Firewalls; antivirus;	Lack of dedicated security personnel
Commercial Bank 2	Viruses; hackers; **disgruntled employees;** system users; suppliers or partners with access to their systems;	Firewalls; encryption; usernames and passwords; antivirus; disaster recovery plans; outsourced	Lack of dedicated security personnel

		security experts; large security budget	

Appendix F: Turnitin Report

Curiginal

Document Information

Analyzed document	Final Report v3.3.9.2.pdf (D101376481)
Submitted	4/12/2021 3:57:00 PM
Submitted by	
Submitter email	theodulus.otieno@strathmore.edu
Similarity	16%
Analysis address	library.strath@analysis.urkund.com

Sources included in the report

W	URL: https://core.ac.uk/download/pdf/148365631.pdf Fetched: 12/10/2020 3:16:52 PM	9
SA	**VERIFICATION.docx** Document VERIFICATION.docx (D40454702)	1
W	URL: https://eprints.qut.edu.au/81626/1/Sarah_Jebb_Thesis.pdf Fetched: 10/31/2019 7:34:19 AM	1
W	URL: https://eprints.soton.ac.uk/381574/1/Final%2520copy%2520of%2520my%2520thesis-2015.pdf Fetched: 11/11/2019 12:05:41 PM	2
W	URL: https://www.standardmedia.co.ke/article/2000068438/kenyatta-national-hospital-digi ... Fetched: 4/12/2021 4:02:00 PM	2
W	URL: https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=7009&context=etd Fetched: 4/12/2021 4:02:00 PM	18
W	URL: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/HerathRao2009_DSS_Pen ... Fetched: 4/12/2021 4:02:00 PM	6
W	URL: https://repository.up.ac.za/bitstream/handle/2263/24117/Complete.pdf?sequence=4 Fetched: 10/19/2020 7:26:51 AM	3
W	URL: https://eprints.qut.edu.au/64070/1/Mohammed_Al_Natheer_Thesis.pdf Fetched: 11/14/2019 6:23:11 AM	34
W	URL: https://repository.uel.ac.uk/download/353398f1bcb3a71a836df15af8c0e2d69285f43abb0e ... Fetched: 4/12/2021 4:02:00 PM	2
W	URL: https://core.ac.uk/download/pdf/193296278.pdf Fetched: 4/12/2021 4:02:00 PM	2
W	URL: https://repository.tudelft.nl/islandora/object/uuid:fa493c67-3a6a-49a3-80c5-2e612d ... Fetched: 10/13/2019 10:53:03 PM	1

URL: https://publications.theseus.fi/bitstream/handle/10024/63254/Fagerstrom_Alex.pdf?s...

1/60

Curiginal

SA	**ICT615_Ass1_RahbarniaA_32718055.docx** Document ICT615_Ass1_RahbarniaA_32718055.docx (D27237098)	1
W	URL: http://130.18.86.27/faculty/warkentin/BIS9613papers/EJIS_SpecialIssue/Myyryetal200 ... Fetched: 4/12/2021 4:02:00 PM	1
J	**The influence of the informal social learning environment on information privacy policy compliance efficacy and intention** URL: a6a8f0c7-9862-4f4b-ac5f-b6785a9307b1 Fetched: 3/13/2019 6:55:26 AM	1
W	URL: https://www.businessdailyafrica.com/corporate/539550-1423034-12mp1as/index.html Fetched: 4/12/2021 4:02:00 PM	1
W	URL: https://www.academia.edu/2664894/Research_on_the_homeless_population_the_particula ... Fetched: 4/12/2021 4:02:00 PM	2
W	URL: https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/3836/2015korovessis10113162p ... Fetched: 10/14/2019 10:51:45 PM	1
SA	**REVISED Master's Thesis - Justus Dircks and Olivia von Sydow.pdf** Document REVISED Master's Thesis - Justus Dircks and Olivia von Sydow.pdf (D40122534)	1