Your topic: Healthcare Data and Information Security Framework

Your desired style of citation: MLA Referencing

Your educational level: Guaranteed First Class

Refrencing Style: MLA Referencing

Number of page: 56

Words: 14000

[Writer Name]

[Subject]

[Date]

Healthcare Data and Information Security Framework in Saudi Arabia

ACKNOWLEDGEMENT

I would take this chance to thank my family, friends and research supervisor for their support and guidance which enabled me to accomplish this task of writing my first dissertation on a topic of my interest and substance.

DECLARATION

Its hereby declared that this document is solely my personal work and that, to the best of my confidence and knowledge, it contains no content formerly published or written through another writer nor material which to a considerable amount has been recognised for the obligation of any other degree or diploma of an University or institution of higher learning, except where due acknowledgement is established.

DEDICATION

My dissertation work is dedicated to my friends and my family. A distinct feeling of thankfulness to my loving partner, whose care, encouragement and reinforcement enabled me to stretch in difficult times and remain focus.

GLOSSARY OF TERMS

IT	Information Technology
HIMS	Health Information Management System
HIS	Health Information System
MOH	Ministry of Health
KSA	Kingdom of Saudi Arabia
USA	United States of America
HIM	Health Information Management
EHR	Electronic Health Records
WHO	World Health Organisation
UAE	United Arab Emirates
COBIT	Control Objectives for Information and Related Technology
PC	Personal Computer
EDW	Enterprise Data Warehouse
PCP	Primary Care Provider
EMR	Electronic Medical Record
PAM	Patient Activation Measure
HIPAA	Health Insurance Portability and Accountability Act
QoS	Quality of Service
VoIP	Voice over Internet Protocol
EHR	Electronic Health Record
LAN	Local Area Network
VPN	Virtual Private Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

DC	Data Centre
DMZ	Demilitarized Zone
ICT	Information and Communications Technology

Table of Contents

ABSTRACT

Healthcare in recent decades has evolved phenomenally with the introduction of patient centre evidence based care. Besides, the new diagnostic and treatment options have enhanced the need and significance of classified patient records. These developments have enhanced the role and need of technology in hospital environment. Growing use of health information systems in hospital has not only facilitated patient care but this system has revolutionised research in health care. However, the use of computer and internet for the online data management of patients also has created patient's privacy and data security issues for hospital management.

Today, the growth of health data standards is somewhat conflicting and overlapping, supporting in market confusion and assisting to growing proprietary intentions. Support by government in standardisation for health data are considered to be important to make credible standards for the coming years, to increase interoperability across the health care industry, and to reduce the hazards related with the performance of non-standard approaches. Supported by the lessons recognised from this research assessing the particular concerns to the implementation of health data standards in the important tertiary hospitals in Saudi Arabia and the views and responses from various officials in the fields of data exchange and standards and medical informatics in Saudi Arabia, a list of approaches needed regarding the growth of national health data standards was established. The aim of this proposed research is to assess security of healthcare data and information security framework in Saudi Arabia so as to identify security risk in the area of end-user, IT security team and IT design.

The method to carry out this study is qualitative. This research will follow a deductive approach and will be and cross-sectional in nature being a study of particular phenomenon at a particular time. This study will utilise the primary data. There are three tools to collect the data a study. These are: participant observation, interview and questionnaire survey. This study will

collected primary data through a survey. The collected data will be analysed and analysed data will be presented along with interpretation in the form of figures and graphs in results and analysis chapter of this dissertation.

CHAPTER 1 INTRODUCTION

1.1 Research Purpose

The purpose of this research is to find vulnerabilities in the health information management system (HIMS) in a healthcare facility and solve them before they are exploited from viruses or hacker attack.

1.2 Research Background

Information security or InfoDec is one of the practicing IT practice that limits the access of data from an unauthorised person or user from using it or disclose it publically. The recodification of data, it perusal, review, copying and destroying of data are all the terms that are used in the working area of Information security. Moreover, information security is now grasping the working system of different working sectors that also includes health care sector.

It can be said that the information technology systems have emerged as an important factor in the routine operation of health care management after have fundamentally changing the dynamics of and control in any business and academia. Kudyba (2010) mentioned that there are many healthcare organisations using Health Information System (HIS) which is especial system use in hospitals to manage patient information such as profile, medical history, Laboratory results, appointments and medicines (pp, 67).

The role of health information systems is to generate, analyse and disseminate timely and reliable data to be used in making health decisions. The ultimate goal of a health information system is to provide information on measures to be taken in the health field. The performance of such a system must be measured not only on the basis of the quality of information produced, but on the evidence of continuous use of this information for improving its authenticity and security (Cholleti, *et al*., 78-84).

Though, health information systems have experienced remarkable improvements, but there are still serious gaps, and much remained to be done to improve their quality and timeliness. In many developing countries, data quality suffers from lack of diagnostic support in peripheral health centres. Healthcare professionals frequently use and manage patient health data often complaint about data quality, difficulty in access to data and its comprehensiveness. The feedback from the central system is often inadequate, which is even more discouraging. Health professionals are likely to wonder whether their reports are published and if so, what effect these publications have (Huser, and Cimino, 145-147).

Few countries have sufficiently effective health information systems even to perfectly master the Millennium Development Goals. Health information systems have been victims of a chronic underinvestment in terms of collection, analysis, dissemination and use of data. Even when available, data is often out dated and unreliable. Unfortunately, this demand of using HIS in healthcare brings a significant risk to patient privacy such as hackers, spies and some types of viruses (Fareed, *et al*., 215-225).

According to Huser, Cimino, (2013) to enable secure and effective information sharing, healthcare institutions need an apparent, reliable capability to recognise information security and decide appropriate handling (pp 98). This is obtained through establishing an information security plan and framework that is inclusive, but flexible sufficient to fulfil modifications in healthcare infrastructure where getting compliance demands. As different institutions have observed, concentrating on one set of compliance demands at a time does not support in making an inclusive strategy or framework; it just enhances the amount of resources and time which institutions have to spend on fulfilling demands. The information security framework must observe at a wide set of security demands comprising particular internal security and privacy demands, business risks, appropriate compliance demands, and business standards.

1.3 Research Problems

Despite the great problem and apparent interest in implementing information security in healthcare in general in both developing and developed nations, we find – particularly in growing countries - that there is a large gap between planning for the introduction of information security to hospitals and the achievement of using these systems and operating them optimally to obtain the primary aim and benefit required and anticipated. This is a particular case for Saudi Arabia, which has its national health care system as the major provider with a rising responsibility and growing contribution from the private sector.

In different growing nations like KSA, people observe that the accessible technology and costs of advanced information technology systems in addition to the lack of technical expertise, technical and computer abilities of hospital staff hospitals, mostly the computer abilities of doctors and members of the nursing staff and technicians, and the lack of facilities for data processing are the major problems to be focused earlier to implementation of hospital information systems. People can add to all these aspects - as defined earlier - the resistance demonstrated through different doctors and health care professionals normally when systems change from the traditional information security units to strict information security in accordance with the latest working system. This issue can be general in both developing and developed nations similarly. Different health care administrators and health information managers are responsive that these changes can take some time to be performed and time is also required to change the doctors behaviours and their views regarding the clinical systems and transform their impressions, attitudes, and beliefs regarding the change of the work context from the old paper to the new technological nature with the important demand to recognise the real purpose behind the desire to change to the previous system which is the most essential thing in the whole subject.

The main problem with the research is the wide research topic of the main theme that focus on the information security all over the international health care sector however, it is important for the dissertation to split the data in accordance with the need of the paper to get accurate results.

1.4 Research Aim

The aim of this proposed research is to assess security of healthcare data and information security framework in Saudi Arabia so as to identify security risk in the area of end-user, IT security team and IT design.

1.5 Research Objectives

- To analyse the concept of health information management
- To analyse the concept of information security
- To explore the current and potential healthcare data and information security risks in hospitals
- To explore the strategies for the protection of healthcare data and information system in Saudi hospitals

1.6 Research Questions

1. What is the concept of health information management?
2. What is the concept of information security?
3. What are the current and potential healthcare data and information security risks in hospitals?
4. What are the strategies for the protection of healthcare data and information system in Saudi Hospitals?

1.7 Rationale and Significance

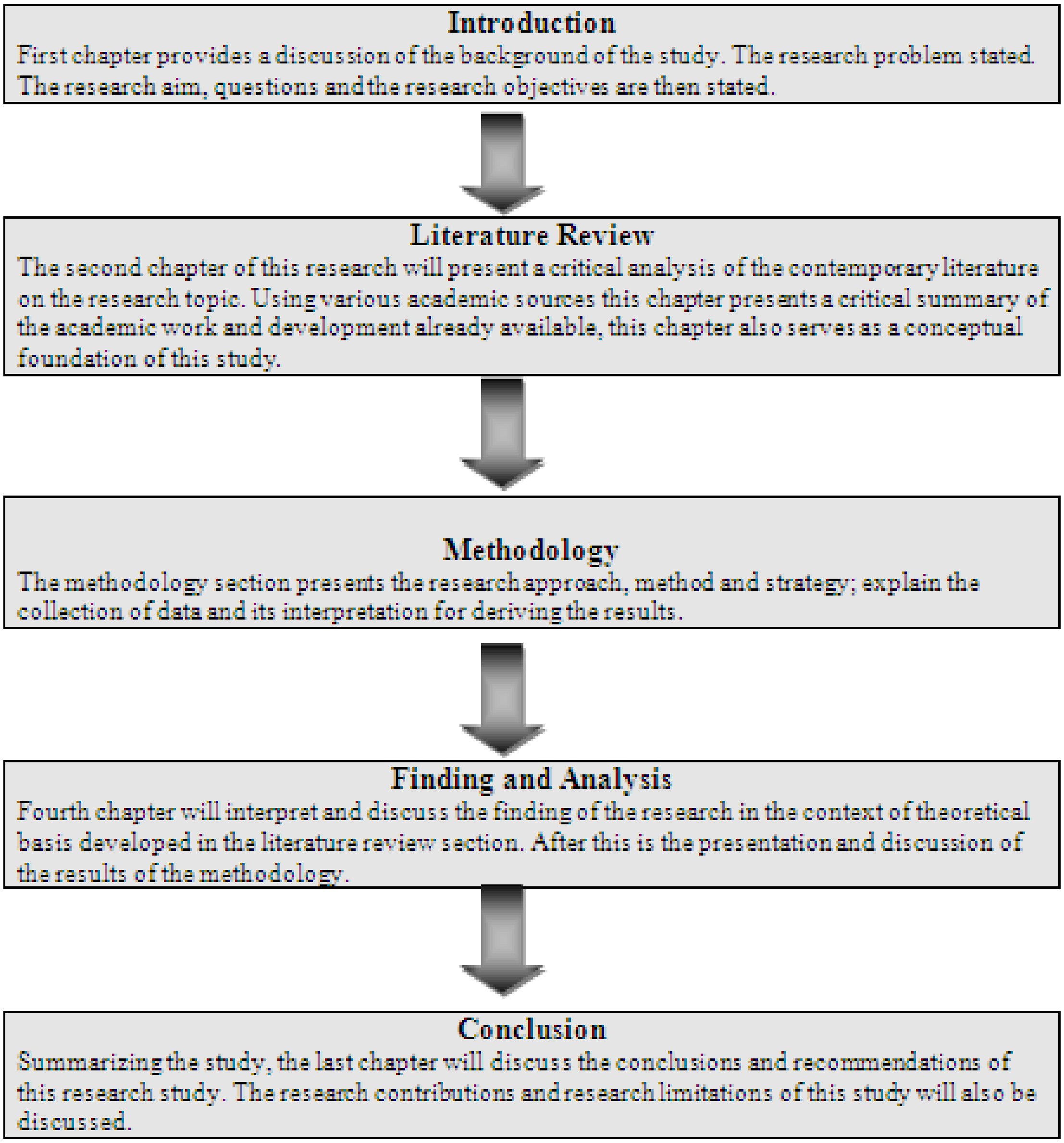
Information is the basis of any reasoned action, any rational and even management, in order to act in the field of public health, it is essential to have reliable information and given in due course. With better quality health information and effective utilisation at national, regional and global levels, it would be possible to improve the evaluation of situations and trends in the health sector, the control of fairness and evaluation of results the health system, and to make more appropriate decisions conducive to the improvement of health (Huser, Cimino, 2013). Recent studies have made it clear that the design of a health policy must be based on an information system to perform data reliably and timely, because only an information system thus allows fulfilling four basic principles in public health know the health status of a population at a given time, put new programs in place, evaluate the changing conditions of the health of a population and inform the public of the risk factors that threaten it (Chen, *et al*., 45-49).

In case of Saudi Arabia, there is some research about information security in the healthcare, and most of these studies focused on the threats to application systems or human threats. Also, when these researches discussed human threats, they focused on misuse of end-users (doctors, nurses and staff) when they are using HIS. In contrast, some researchers have overlooked the role of IT security engineers in creating various data security risks and issues (Abdelhak, *et al*., 67-75).

There is though little evidence that IT security engineers also are responsible for some problems and issues when it related to IT security design or misuse IT systems and applications. For instance, in the USA applications of Kaiser Permanente Medical sent more than 800 email messages from nurses and pharmacists to the wrong people and then the blame was placed on a technical glitch that occurred after the installation of new software (Shoniregun, 225-235). Hence an inquiry with a deliberate focus on operational divisions such as IT design, IT engineering and end user will bring a precise and explicit assessment of current HIMS risks in Saudi hospital and such a deeper understanding would facilitate hospital management, Saudi health officials and healthcare sector to better strategies and protect healthcare data in hospitals.

1.8 Proposed Structure

This proposed research will follow the standards dissertation structure described below:



Introduction

First chapter provides a discussion of the background of the study. The research problem stated. The research aim, questions and the research objectives are then stated.

Literature Review

The second chapter of this research will present a critical analysis of the contemporary literature on the research topic. Using various academic sources this chapter presents a critical summary of the academic work and development already available, this chapter also serves as a conceptual foundation of this study.

Methodology

The methodology section presents the research approach, method and strategy; explain the collection of data and its interpretation for deriving the results.

Finding and Analysis

Fourth chapter will interpret and discuss the finding of the research in the context of theoretical basis developed in the literature review section. After this is the presentation and discussion of the results of the methodology.

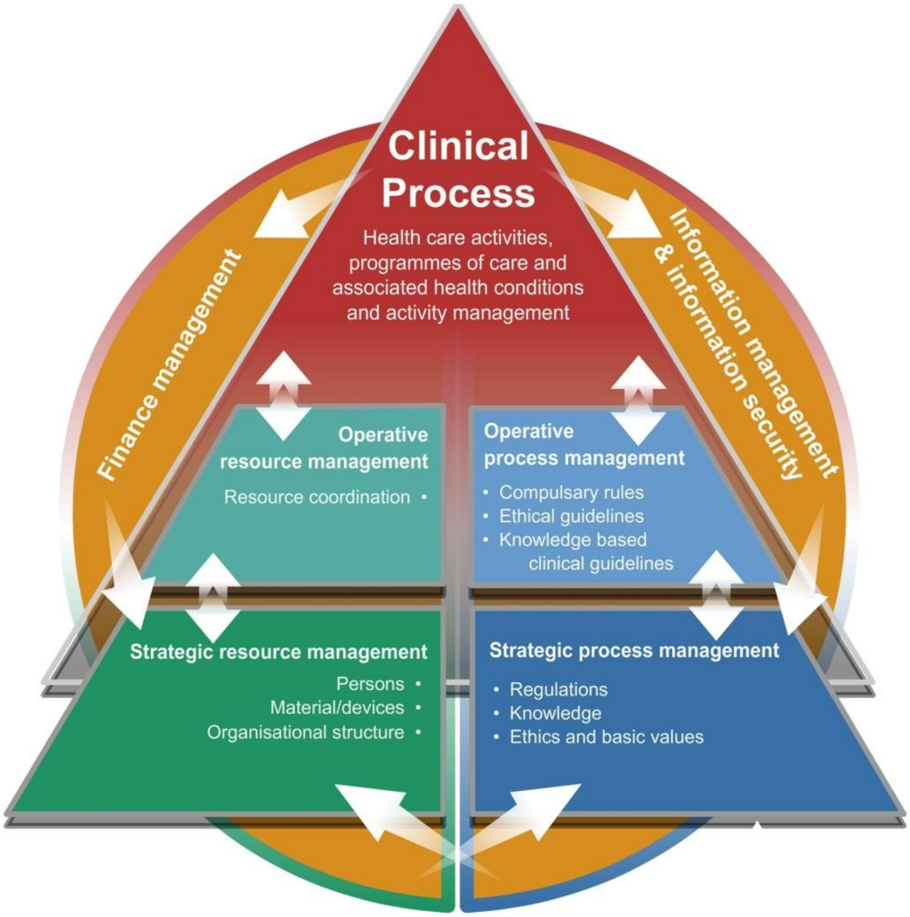
Conclusion

Summarizing the study, the last chapter will discuss the conclusions and recommendations of this research study. The research contributions and research limitations of this study will also be discussed.

CHAPTER 2 LITERATURE REVIEW

2.1 The Concept of Health Information Management

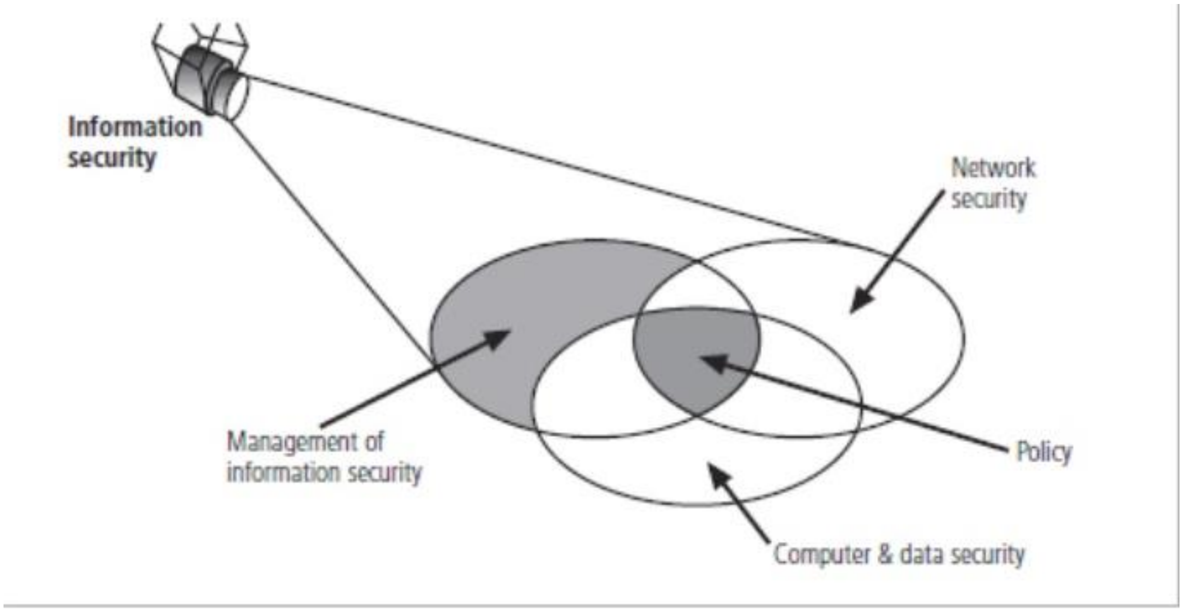
The communities, regions, and countries that comprise the growing world face different health-associated challenges, and the health systems that focus those challenges are trying with limited capability and resources. Therefore, health leaders should concentrate on increasing the value of scarce resources and getting approaches to make health systems operate as competently as possible (Huser, Cimino, 89-95). Having trustworthy information on the performance of various parts of the health information management and security is the single method to devise, execute, and observe health interventions. Productive strengthening of health information management will need timely, relevant, and perfect information on the performance of the health information management system itself.


Clinical Process
Health care activities, programmes of care and associated health conditions and activity management
Finance management
Information management & information security
Operative resource management
Resource coordination •
Operative process management
• Compulsary rules
• Ethical guidelines
• Knowledge based clinical guidelines
Strategic resource management
Persons •
Material/devices •
Organisational structure •
Strategic process management
• Regulations
• Knowledge
• Ethics and basic values

The 21st century has been called upon Information Technology in reaching impressive levels of development. Constantly alluded to the information society, conceived as a form of economic and social development in the acquisition, storage, processing, evaluation, transmission, distribution and discrimination of information with a view to the creation of knowledge and satisfaction the needs of people and organisations, plays a central role in economic activity, wealth creation and the definition of quality of life and cultural practices of citizens. Changes of modernity in the political, economic, cultural and technological order have caused that information management is developed and it depends on the complexity of the organisational development of an institution where knowledge management is necessary and indisputable.

The information security in health care is increasingly maintaining more space in the economies of countries international. Thus, there is a close relationship between the management of information and knowledge and the quality of the work in health care organisations in regards of information security. Taking into account that technologies are necessarily means for transmitting and managing knowledge and information, as essential for development within each organisational element.

With the emergence of the theory of organisation, the importance of information deepened. An organisation is made up of people, material resources and information, so organisations should be considered as information systems system. This work requires numerous concepts and highlights the importance of information management as the natural support of knowledge management and organisational learning through the role of new information technology and knowledge and their role to bring forward the organisational change. Hence, it becomes necessary to highlight the importance of the process of managing information and knowledge for work criteria change in health care organisations, a subject on which we have developed this paper.

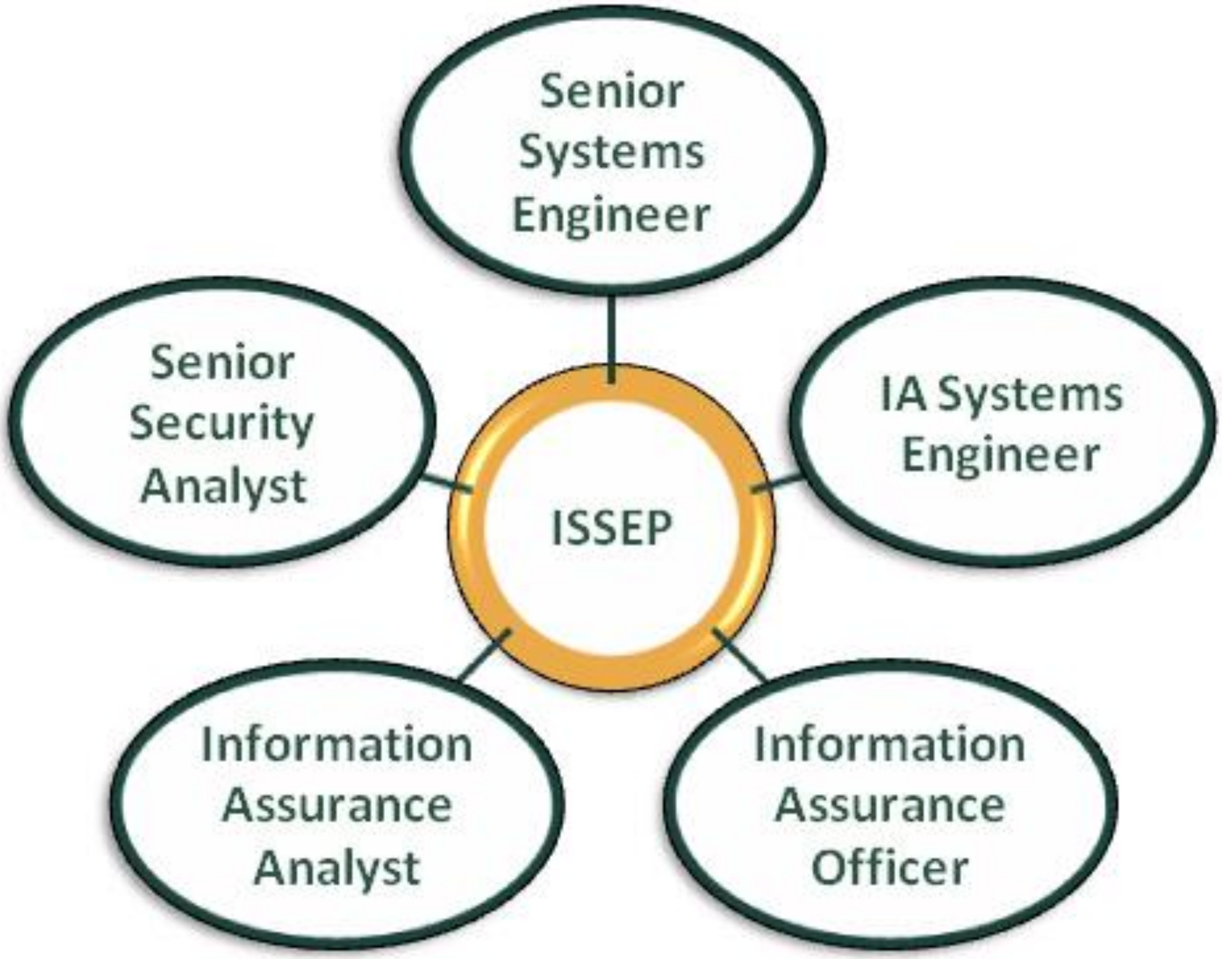


Components of Information Security

A vital resource in any health care organisation today is the incorporation of new technologies and tools that provide working and security intelligence in providing information products it has been a great challenge and an opportunity for information science and the modern health care business world, which takes as an important concept knowledge management and information. With the emergence of the theory of healthcare organisation, the importance of information deepened. A healthcare organisation is made up of people, material resources and information system. The latter determines the "order and chaos" among individuals, resources and the interplay resource persons. For this reason, organisations should be considered as information systems.

The impact of economic, political, cultural, technological and other changes has led to a revolution in information management in health care organisation, rules, concepts, procedures, behaviour, and products and services are then transformed a new attitude permeates the daily life of the projection and the development of information activities; arguably the new management model has the indispensable basis of knowledge management has raised the immediate need to implement models for total quality management in institutions of information, suggests the close relationship between information management, knowledge and quality in the work of a health care organisation.

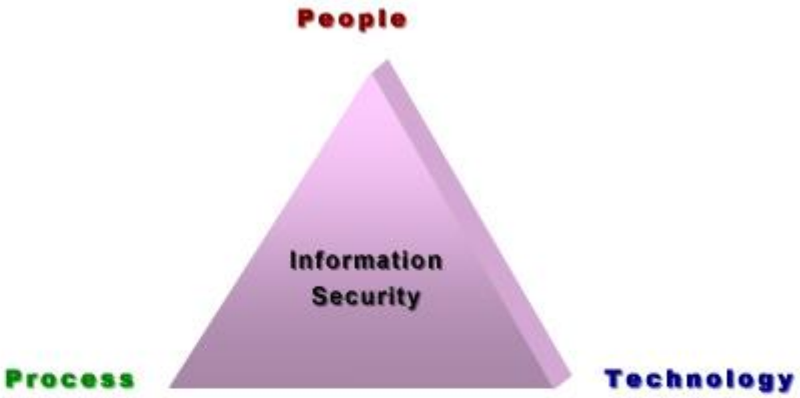
It is known as the set of coordinated management to lead an organisation, this being the conglomerate of people and facilities with provision, responsibilities, authority and relations activities. When speaking of information institution is alluded to a knowledge organisation, which, through a set of processes managed capabilities and provides, to the extent that this knowledge management increases, the organisation gains in development and is, itself generates positive changes. Knowledge is a process of organising and integrating reasoning of thought which is useful, considering also that is a set of information, rules, and interpretations from organisational experience, either individually or collectively.



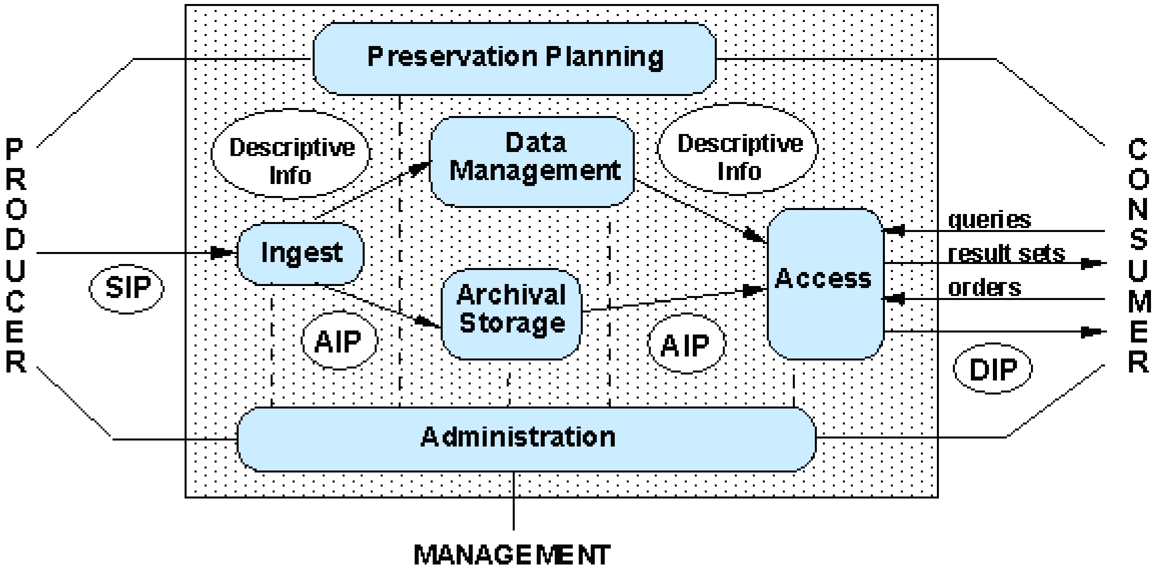
Therefore, in organisational management level information would include all activities relating to the production of solid, viable, reliable, and updated information that will determine the decision-making process in a healthcare organisation. Information services as an essential part of the infrastructure for knowledge management, supply information, promote the generation of knowledge for finding solutions to problems facing organisations, analyse their impact on business performance and influence the behaviour of individuals to information. The information security is linked to the generation and implementation of strategies, the establishment of policies and the development of an organisational and social culture aimed at rational use efficient, effective and information in accordance with the objectives and goals companies in performance and quality.

Current strategies for managing information and knowledge should respond to the new types of claims resulting from the emergence of more modern management trends in healthcare organisation. In the creation of new systems of information security is essential to consider factographic sources (data), documentary and non-documentary, computer systems, culture of information, communication patterns, among others.

Depending on knowledge management and managing information ensures greater customer satisfaction since to service excellence, based on the mission and vision of the organisation, ensuring market competitiveness. Those who manage to develop a sound and efficient management of knowledge materialise their potential to unite and generate feelings of identity, sensitivity to learn and adapt to changing environmental conditions. To achieve all the above knowledge management should be used by systematic use of external information in any industrial and working sector especially in healthcare organisation.



Knowledge management seeks to ensure that the healthcare organisation has the information and skills necessary for continued internal and external environmental changes adaptation. Proper management of information and knowledge depends to a large extent, the implementation of quality management. Information moves environmental organisations through formal and informal networks (Abdelhak, et al., 415-425). Its infrastructure is visible and defined, consisting of cables, mailboxes, addresses etc. Information as a fundamental principle has a meaning and can nourish to the receiver and implies that, to transform data into information, add value in several ways. The most common ways are running contextualising to know for what purpose were generated; categorising for the units of analysis of the main components; calculated by mathematical or statistical analysis; correcting errors and condensing to summarise more concisely. Throughout the strategic planning organisation that includes information management, so as to guarantee the fulfillment of the mission and vision of the Organisation which is important how you visualise the desired changes in the healthcare institution and planning the alternatives carried out.

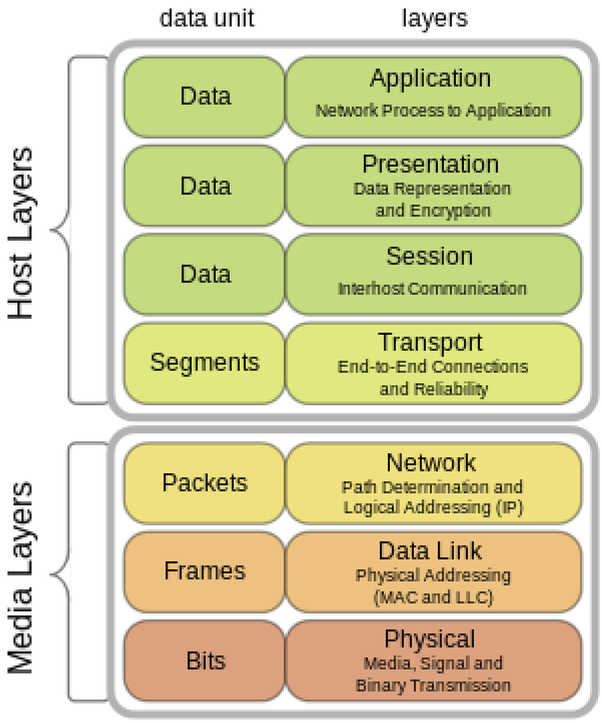


Source: Procedures Manual for the Consultative Committee for Space Data Systems (2001)

Health information management (HIM) and information security is the practice of obtaining, examining and securing traditional and digital medical information imperative to render timely and quality care to patients (Abdelhak, *et al.*, 67-78). McKibbon, *et al.*, (2012) suggest that traditional (paper-based) records with the extensive computerisation of health data are being substituted with Electronic Health Records (EHRs) (pp 108). The tools of health information technology are being utilised increasingly to enhance effectiveness and efficiency in the practices of information management in the various health care facilities. Both health human resources information systems (HRHIS) and hospital information systems are general applications of HIM (McKibbon, *et al.*, 102-105).

As per World Health Organisation (WHO) the appropriate gathering use and management of data in healthcare facilities will determine the effectiveness of healthcare system in identifying health problems, setting priorities, and developing innovative solutions and resources allocation to improve quality of healthcare interventions (Abdelhak, *et al.*, 105-115).

Saudi Arab started supporting its health information management system with an assessment of the weaknesses and strengths of current information management systems, sharing outcomes with all stakeholders (Abdelhak, et al., 49-54). All were confirmed on the demand for transformation of different vertical programme-particular information systems into an inclusive, decentralised, integrated, and action oriented simple method.


data unit
layers
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Media Layers
Packets
Network
Path Determination and Logical Addressing (IP)
Frames
Data Link
Physical Addressing (MAC and LLC)
Bits
Physical
Media, Signal and Binary Transmission

As a first stage about design and conceptualisation of the system, a minimum set of signs recognised and a plan was established for making a system in the nation. The design concentrated just on the use of information in management, planning, and the development of coverage and quality of services. All health and support staffs were trained, using a training of trainers cascade method. Health information management and use was comprised into the pre-service training course and the job details of all health staffs and support staffs. Quarterly feedback, supportive management visits and yearly reviews were established. A mid-term assessment of the accomplishments of the health information management system observed it to be one of the best in KSA. For the first time in KSA, the health sector has information by facility by month. However, very little development has been observed in use of information in rationalising decisions. The assumption is that, no matter how good the design of a health information management system, it will not be productive unless there is internal dedication, desire, and dedication of leadership to have an efficient and effective health information management system.

2.2 The Concept of Healthcare Data and Information Security

The accumulation of information is a necessity of modern societies in all its manifestations. The information is essential to effectively perform all tasks to which they must respond daily. Without exaggeration that without the accumulation and circulation of information modern societies would be paralysed in its many activities. The collection of information has multiple projections and all its contents to be preserved. If the information is about people, namely, refers to personal data must undergo controlled rules and principles and not to cause injury to the rights of individuals. If that information also includes disclosures on health, i.e. data become health-guarantees must be tightened. Data on health is an intrinsic and essential element in the life of a person (Murdoch, Detsky, 39-45). Adequate health care requires accurate information on aspects of life and health of the patient and a perfect preservation of the same. Along with the specific interest of each in their own health, it is a social good that the state has to promote and preserve by prevention campaigns and vaccination or through research.

These social aspects of health also require the use of patient data; use to be conducted with appropriate controls to avoid injury to their rights and interests. The need to control the information that reveals aspects of a person's health is paramount to keep intact their enjoyment and exercise of fundamental rights of the individual and avoid depriving the person of his dignity as a human being. Adequate health care requires us to disclose medical professional extremely sensitive data, aspects of our life that normally would not disclose to anyone except in the case of game found in our health, why must be particularly protected. Therefore, the respect for the rights of individuals must be referred to a level equivalent to the need to preserve our health protection.

2.3 Healthcare Data and Information Security Risks in Hospitals

Healthcare organisations deal with sensitive and huge of patient data and employee’s information which is usually caused a risk or issues with reliability, security and privacy. More than 1.5 million names were exposed because data breaches from 2006 to 2007 which happened in healthcare organisations only. Most of the violations of security in the healthcare are coming from authorised end-users and are arising due to mistake, misuse or for other reasons. For that, the threats to the healthcare organisation can be either from inside or outside the healthcare organisations. Threats to healthcare organisations can divide in two types: the internal threat which includes attitudes and behaviour of employees regarding data safety such as carelessness, lack of awareness, rushing without reasons and exchange of password between the employees.

The second type of threats to healthcare organisation is external threats which include risks that coming from outside the healthcare domain such as viruses, malware and hackers. Therefore, Information security in healthcare is increasing in demand and responsibility because many of the healthcare organisations spend large money on their IT revenue in trying to close vulnerabilities and mitigate threats and intrusions. Healthcare organisation spends an average of 2.7 % of its budget on IT. The poor of security in healthcare organisations might be lead to potential threats and Lose and maintain the confidentiality of patient information.

Another major risk to health information data is from cyber criminals. For web offenders, there are several levels of motivation. First, industrial espionage: it steals the pharmaceutical laboratory data on research or medical advances. Encryption is also reported in France: hackers encrypt computer data of health facilities and decrypt them against a certain sum of money. Another motivation for cyber criminals is the resale of health information to complementary insurance companies and laboratories. The medical information of individuals can be valuable for insurers: they allow them to adjust prices more accurately. As for the pharmaceutical industry, they could establish statistical significance of capitals with this information in order to guide the marketing of medicines.

2.3.1 The Saudi Scenario

The management and delivery of health services in Saudi Arabia is a complicated target. Saudi Arabia spans a large geographical region with fragmented healthcare methods whose care quality is not same particularly between its scattered and diverse areas. The Ministry of Health (MoH) is the major government institution supported with the provision of preventive, curative and rehabilitative medical facilities. Its tasks comprise strategic planning, making particular health policies, managing all health service delivery plans, and observing and managing all other health-associated activities. Though, inception of health services in Saudi Arabia took position half decade earlier, particularly in 1950, when the first campaign against malaria was established. After this, in the Kingdom, the healthcare system developed constantly until 1980 when there was a time of fast development in each sector in Saudi Arabia because of to the enhancement in financial wealth. In the early 1980s, the perception of primary healthcare became famous and the health sector structure began to become apparent. At presently, the MoH runs a three-tier healthcare network which comprises primary, secondary and tertiary levels; these correspond to health centres, general hospitals and specialist hospitals respectively.

The Saudi Arabian health system is undergoing a period of change. Such situations are opportunities to improve the sector, given the political will to bring about change. Among the weaknesses of the information system the low ratio of maintaining patient's digital data is found in various reports. In connection with this point an absence in the culture of generation, exchange, use and feedback of information was observed. Interested institutions do not articulate their processes and seek to align their interests to optimise the functions required for the proper functioning of the information system.

The King Fahad Hospital has developed a culture of reporting, since it has been possible to demonstrate the importance of reporting for surveillance. Resistance to change and reluctance to share information is one of the main threats facing the health information system. Political change and the abandonment of the initiatives is also an incentive for potential impediment to the adoption of information technology in the sector.

The Ministry of health in Saudi Arabia and King Fahad hospital has been making a significant effort in establishing a data warehouse to integrate the various sources of information. However, they still have very low levels of integration and capturing procedures are wasteful, the information is duplicated in some cases and not in others is reported. Furthermore, there is a feedback mechanism that includes an acknowledgment and suggestions for improvement. In King Fahad Hospital records of births and deaths has been able to develop a culture of gathering and managing data on computers , but there is a long way to go with other information (Khalifa, 49-59).

Computerisation of health data requires a lot of reliable information and use cost-effectiveness of the technologies. This is more critical because a systematic management of health data in Saudi Arab is pivotal for effectively meeting the health service needs of the population and introduce new treatment interventions. The digitisation of clinical histories demands a substantial improvement of infrastructure, especially in rural areas of Saudi Arab because health care facilities in these areas are short of essential resources for HIMS such as access to internet, data management department and trained IT staff.

In addition, there is a need to take into account issues of privacy and confidentiality of the existing information contained in medical records in these areas. The first step towards digitisation of health data in the remote area is to shift current health data on computer from papers and then install the systems and provide staff to collect new data electronically and the third step should be to make this data available at regional and national level.

2.3.2 King Fahad Medical City

King Fahad Medical City is considered the largest and most advanced medical complex in the Middle East with a total capacity of 1095 beds. Enjoying the strategic location in the heart of Riyadh City, the capital of Kingdom of Saudi Arabia, it comprises of four hospitals expected to treat annually more than 50,000 in-patients and over 600,000 out-patients. With the strategic partnership with NVS-Soft (it’s a UAE-based firm which provide information management solutions for the North African and Middle East markets), King Fahad Medical City is fast forwarding towards a paperless future with electronic medical records where information is easily accessible and secure.

2.4 Strategies for the Protection of Healthcare Data in Saudi Hospitals

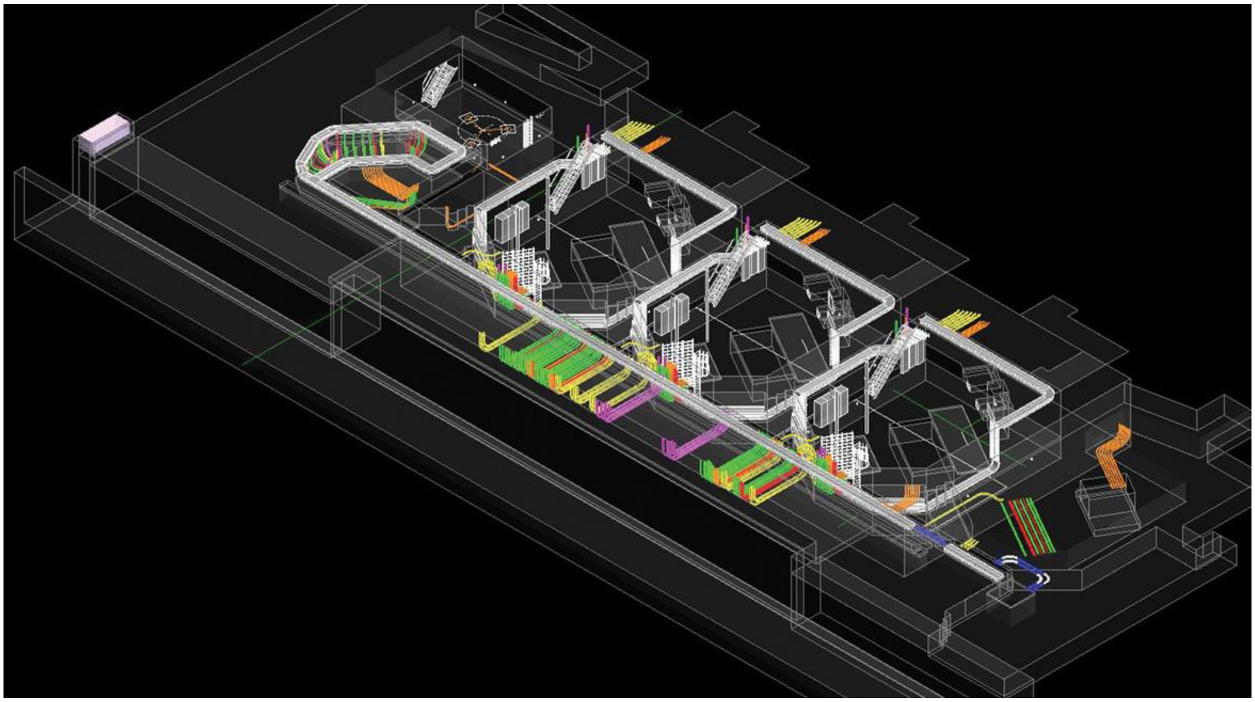
The efficient and secure use of healthcare data requires training, experience and education of the user, and procurement of user friendly and well protected computer programmes so that the doctor and health researcher can easily uses the computerised with confidence to accomplish with diagnostic and therapeutic targets. Besides, these computer programs must be customised to the need of health related decision making, such as easy and safe access to individual patient data for the clinical practices, systematic record of numerous patient of various therapeutic segments so that health researcher can use it in research etc. However, the key of data security lies that every person or institution has an easy accessed to required data but no one else without authorisation can reach to data beyond the scope of their work (Abdelhak, *et al.*, 149-159).

Clinical experience and knowledge of computer application allows the clinician to interpret the information yielded by the system and apply it at the right time. Likewise, IT engineers recognise system errors and decide when to omit inconvenient or irrelevant information. These characteristics define the appropriate user applications in Medical Informatics. The appropriate user should combine deep knowledge of medicine and clinical experience with the knowledge of the application and objectives. To meet these requirements, training and understanding of computer basics is required.

The concept of an authorised user the appropriate system routes cam meet the objective of data protection while ensuring that everyone has easy access to relevant data within the scope of their task. This is more important because patient data and other medical records can spiral out of control of the user and does not necessarily depend on the design of the computer system. In protecting the confidentiality and privacy of medical records there is a need to bring a balance between access to information, compliance with clinical objectives and application of appropriate user role in the protection of clinical data (Wilkowska, Ziefle, 49-51).

2.5 Do healthcare organisations implement Information security standards?

Although Information security assumes an essential part in ensuring the information and resources of an association, frequently there is some news about security events, for example, destruction of sites, server hacking and information spillage. Associations should be completely mindful of the need to give more assets to the assurance of data resources, and Information security must turn into a top concern in government and organisations and for the human services associations. Data Security is the security of data and data frameworks from unapproved access, use, divulgence, disturbance, change or devastation. Data Security is accomplished by guaranteeing the privacy, uprightness, and accessibility of data. In health awareness, and for the reasons of this aide, privacy, honesty, and accessibility mean:



Privacy: The property that electronic health care data is not made accessible or revealed to unapproved persons or procedures.

Uprightness: The property that electronic health care data have not been modified or obliterated in an unapproved way.

Accessibility: The property that electronic health care data is open and useable upon interest by an approved individual.

It is exceptionally important for social insurance associations to execute security guidelines keeping in mind the end goal to keep from any abuse or loss of data. Gauges, for example, Control Objectives for Information and Related Technology (COBIT) and information security principles are essentially connected and executed in social insurance associations. E.g. the baseline of COBIT Security concentrates on the particular hazards around IT security in a manner that is easy to take after and actualise for little and vast associations

Surveying the electronic health care data privacy, dependability, and accessibility needs the association to first comprehend their practices health care IT environment. This may incorporate the advances the association's practice sends for both clinical and regulatory purposes, where those advancements are physically utilised and found, and how they are utilised inside of their practice. As they evaluate their health care IT environment, consider those circumstances that may prompt unapproved access, use, divulgence, disturbance, change or obliteration of electronic health care data. In this manner it has been watched that social insurance associations execute Information security benchmarks.

2.6 Knowledge of Security Equipment

Security equipment named "high" must not just be ensured against ecological hazards, for example, flames, flooding, temperature varieties, and so forth. In health awareness security equipment ought to be actualised so that the key data is defended and information misfortune can be anticipated. Grouping of equipment ought to be taking into account hazard appraisals. Data delegated "delicate" must not be put away on compact PC equipment such as tablets, PDAs, memory sticks, and so forth. On the off chance that it is important to store this data on versatile equipment, the data must be secret key secured and encoded in consistence with rules from the IT division.

2.7 Lack of experience in the new threats and ways of attackers

These days, utilising data frameworks as a part of the health awareness environment gives numerous potential advantages, for example, enhancing the nature of consideration, lessening medicinal blunders, improving the decipherability, accessibility and openness of data. On the other hand, Healthcare Information Systems (HIS) security hazards have expanded fundamentally lately. Essentially, HIS are undermined by both incidental occasions and purposeful activities hazards, which can seriously harm health care data frameworks' unwavering quality and thusly debilitate experts of future utilisation.

Assailants exploit system gadgets turning out to be less safely arranged over the long haul as client’s interest special cases for particular business needs. Now and again the exemptions are conveyed and after that left fixed when they are no more material to the business needs. Now and again, the security danger of the special case is neither legitimately broke down nor measured against the related business require and can change after some time. Aggressors look for defenceless default settings, electronic openings in firewalls, switches, and switches and utilise those to enter safeguards. They endeavour blemishes in these gadgets to get entrance to systems, side-track activity on a system, and capture data while in transmission. Through such activities, the aggressor gets entrance to touchy information, modifies essential data, or even uses a bargained machine to stance as another trusted framework on the system.

It has been observed that lack of experience in handling threats is itself a serious threat to information system as new threats and ways are effecting the health care organisations from quite recently. However, it is therefore very imperative for the security engineer to apply and implement international standards of Information security in the organisation to prevent from mishaps.

2.8 Change Management Policy of Project

Guaranteeing that health care data is shielded from unapproved exposure and protected to avoid unapproved adjustment or annihilation is a key essential for actualising PC based patient record frameworks. In view of the assorted qualities of the hierarchical issues and the specialised intricacy of the frameworks and systems, securing health care data can be accomplished most adequately with an association wide program. At first change is clumsy yet it is something that presses the administration out of the safe place. Transforming starting with one states then onto the next miracles our control over results and is uncomfortable. Be that as it may, it is still imperative to actualise changes in the matter of the Information security of an association. What's more, the rate of progress in human services is quickening, not abating and the effective powers that are changing social insurance can produce limitless financial potential for the individuals why should capable utilise powerful survival procedures in the fleeting and in the meantime anticipate achievement extendedly.

The Information security supervisor must be cognizant to ceaseless changes in the dynamic medicinal services environment. Medicinal services hierarchical structures are evolving. Group and provincial health care frameworks and systems are being shaped. Legitimate and accreditation necessities for ensuring patient security are evolving. Security innovation is developing quickly. The establishment of PC based patient record frameworks and systems direct assessing hazards, deciding framework and system security necessities, and executing suitable controls.

2.9 Training to Develop Security Skills

Information ruptures and distinguish robbery have apparently happened since data has been put away and used in current times. As the way of data has moved from printed copy structures and print materials into advanced arrangement put away, got to and transmitted over the globe in barely a second, the simplicity in which that data is utilised and abused has changed drastically. With these critical changes, security architects ought to prepare the related staff and create security aptitudes so if there should be an occurrence of any bizarre circumstances, data could be made secured.

A fruitful IT security system comprises of: 1) creating IT security approach that reflects business needs tempered by known hazards; 2) educating clients of their IT security obligations, as reported in office security strategy and strategies; and 3) setting up procedures for checking and exploring the project. 6) Security mindfulness and preparing ought to be centred on the association's whole client populace. Administration ought to set the sample for fitting IT security conduct inside of an association. A mindfulness project ought to start with an exertion that can be conveyed and executed in different ways and is gone for all levels of the association including senior and official directors. The viability of this exertion will ordinarily focus the adequacy of the mindfulness and preparing project. This is additionally valid for a fruitful IT security program.

2.10 Who has authority to change the network configuration?

All new arrangement administers past a pattern solidified design that permit movement to course through system security gadgets, for example, firewalls and system based IPS, ought to be reported and recorded in a setup administration framework, with a particular business purpose behind every change, a particular singular's name in charge of that business need, and a normal span of the need. The overseers need to analyse firewall, switch, and switch arrangement against standard secure setups characterised for every sort of system gadget being used in the association. The security setup of such gadgets ought to be archived, investigated, and sanction by an association change control board. Any deviations from the standard design or overhauls to the standard setup ought to be reported and sanction in a change control framework.

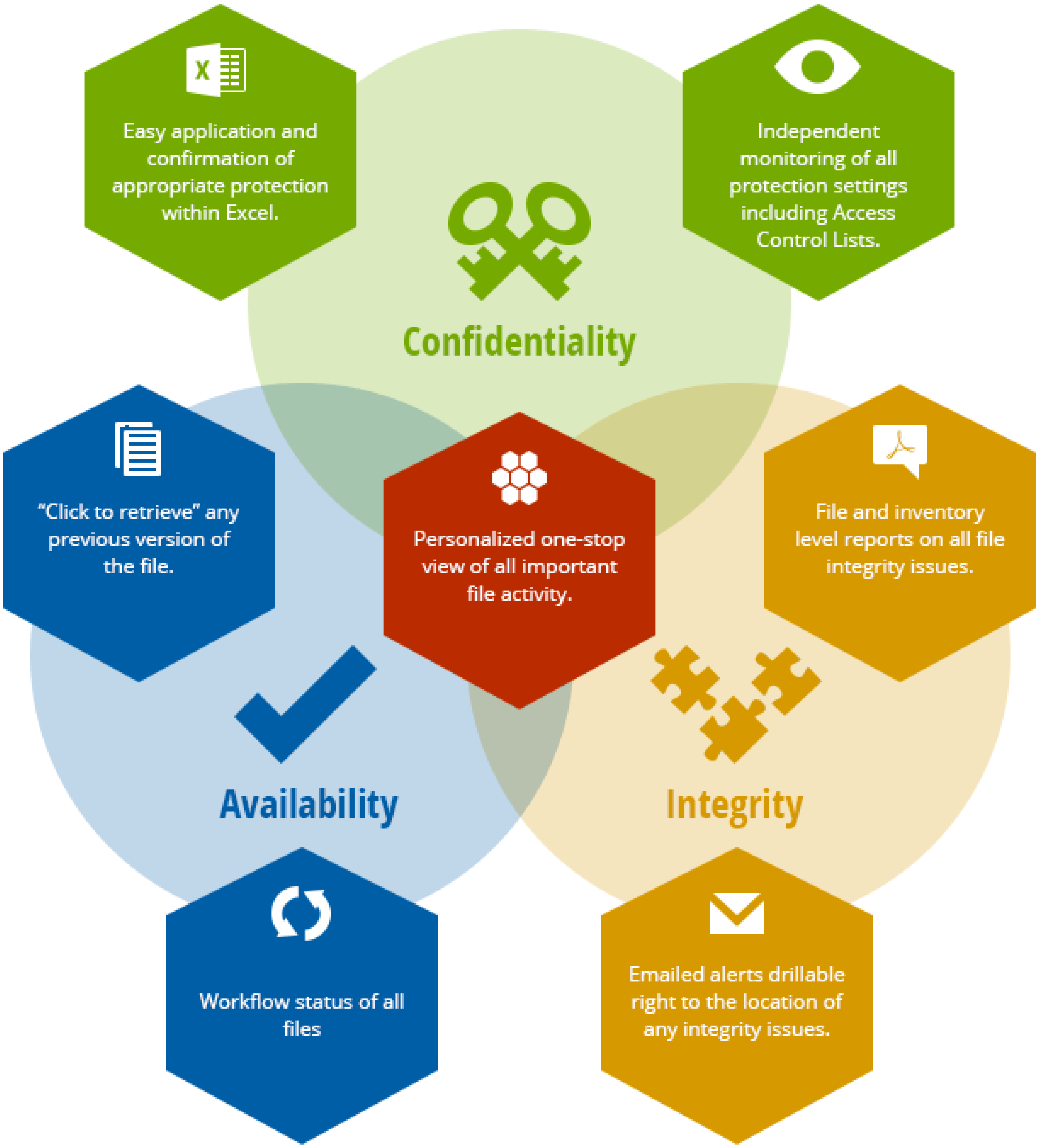
However, network administrators or higher officials have the authority to change network configurations. They utilise computerised instruments to confirm standard gadget setups and identify changes. All changes to such records ought to be naturally answered to security staff

2.11 End-user when using data in healthcare

Usage of data information system in Healthcare

Karlsson (2014) characterize protection or confidentiality as the privilege "to be not to mention". As per him, it is the privilege of people to keep data about themselves from being uncovered to others; the case of people to be left to figure things out without anyone else's input, from reconnaissance or impedance from different people, associations, or the legislature. The data that is shared as an aftereffect of a clinical relationship is viewed as private and must be ensured. The data can take different structures (counting recognizable proof information, findings, treatment and advancement notes, and research facility comes about) and can be put away in various media (e.g., paper, feature, electronic documents). Data from which the character of the patient can't be learned—for instance, the quantity of patients with prostate malignancy in a given clinic—is not in this classification.

Understanding data ought to be discharged to others just with the persisting’s authorization or as permitted by law. It can be said that the doctors cannot access to patient data. Data can be discharged for treatment, instalment, or authoritative purposes without a persisting's approval. The patient, as well, has government, state, and lawful rights to view, get a duplicate of, and correct data in his or her health record.


Easy application and confirmation of appropriate protection within Excel.
Independent monitoring of all protection settings including Access Control Lists.
Confidentiality
"Click to retrieve" any previous version of the file.
Personalized one-stop view of all important file activity.
File and inventory level reports on all file integrity issues.
Availability
Integrity
Workflow status of all files
Emailed alerts drillable right to the location of any integrity issues.

The way to secure the privacy is verifying that just approved people have admittance to data. The procedure of controlling access constraining that can see what starts with approving clients. In a doctor rehearse, for instance, the practice executive recognizes the clients, figures out what level of data is required, and relegates usernames and passwords. Essential benchmarks for passwords incorporate obliging that they be changed at set interims, setting a base number of characters, and disallowing the reuse of passwords. Numerous associations and doctor practices take a two-level way to deal with validation, including a biometrics identifier output, for example, palm, finger, retina, or face acknowledgment.

The patients' entrance is in light of pre-established, part based benefits. In a doctor rehearse, the medical caretaker and the secretary, for instance, have altogether different assignments and obligations; hence, they do not have entry to the same data. Consequently, assigning client benefits is a discriminating part of therapeutic record security: all clients have entry to the data they have to satisfy their parts and obligations, and they must realize that they are responsible for utilization or abuse of the data they view and change.

Under the Health Insurance Portability and Accountability Act, Privacy and Security Rules, organizations are considered responsible for the activities of their employees. Workers of the UCLA wellbeing framework were found to have had admittance to famous people's records without fitting approval. UCLA neglected to "execute efforts to establish safety adequate to lessen the dangers of impermissible access to electronic ensured wellbeing data by unapproved clients to a sensible and proper level". The wellbeing framework consented to settle protection and security infringement with the U.S. Bureau of Health and Human Services Office for Civil Rights (OCR) for $865,000. Controlling access to wellbeing data is vital yet not adequate for ensuring secrecy; extra efforts to establish safety, for example, broad preparing and solid protection and security strategies and techniques are crucial to securing patient's health records.

It is stated that the information utilisation holds great potential for the healthcare sector to empower health care frameworks to deliberately utilise information and investigation to recognise inefficiencies and best practices that enhance the information system in healthcare organisations. A few specialists believe that the chances to enhance healthcare and effective information security system simultaneously could apply to as much as 30% of general social insurance spending. This could be a win/win generally. However, because of the unpredictability of health awareness and a slower rate of innovation appropriation, healthcare industry lacks behind these others in executing compelling information withdrawal and explanatory methodologies (Höne & Eloff, 78-85). Like investigation and business knowledge, the term information mining can mean distinctive things to diverse individuals. The most essential meaning of information mining is the investigation of substantial information sets to find examples and utilise those examples to estimate or anticipate the probability of future occasions. Moreover, not all investigations of vast amounts of information constitute information mining as it is comprehended. Usually experts categorise the analytical parts of the information data system as,

- **Descriptive analytics**— it usually evaluates the current and previous working in the data information system in healthcare system
- **Predictive analytics**—furthermore, the analytical model predict possibilities for the future of healthcare organisation's information framework on the basis of previous descriptive
- **Prescriptive analytics**— Prescriptive analytics helps the project managers to evaluate recommendation for the management of the healthcare organisation in order to adopt different precautions that might work as risk management plan for the organisation in maintain the balance of working in organisation.

It is seen that the use of Information security framework in the end-users of healthcare organisation includes revealing examples from tremendous information stores and utilising that data to manufacture prescient models.

However, information security framework in healthcare organisation in the current business environment stays, generally, a scholarly practice with just a couple of logical examples of overcoming adversity. Academicians are utilising information mining methodologies like choice trees, groups, neural systems, and time arrangement to distribute research. Human services, on the other hand, have dependably been moderate to join the most recent exploration into ordinary practice as it is explained in the report.

However, research the information security of end-users in an healthcare organisation, it is observed that the information security of the end user in an organisation are usually violated that it is the policy of most of the company to save the passwords of employees and other participants on their server and it is a continuous threat to their employees that their data might be used by other people publically. Therefore, it is important for the maintained the stability of the end-user’s data in order to maintain their loyalty and confidence that normally lack in the normal employees of the organisation especially in any health care organisation.

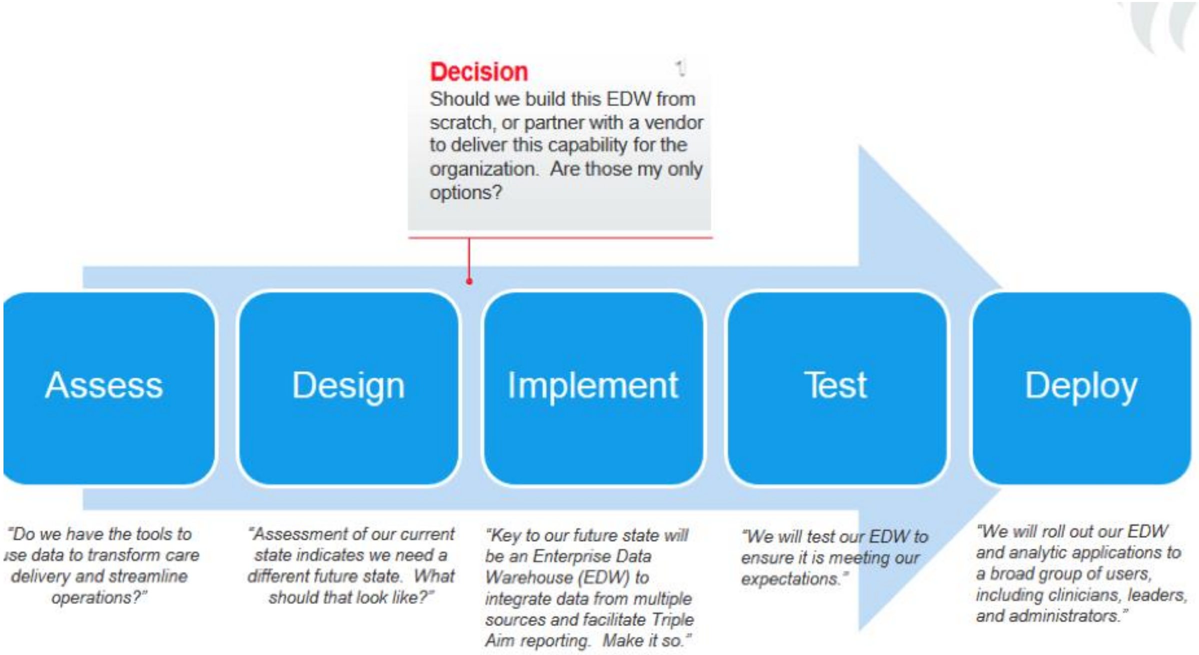
2.12 Different system approaches use for data information system

The effective strategy for handling information authorisation in the end-users of organisation past the domain of scholastic examination is the three frameworks approach. Actualising each of the three frameworks is the way to driving true change with any examination activity in healthcare organisation. However it is unfortunate that not many healthcare associations execute every one of the three of these frameworks.

The three frameworks are:

The investigation framework

This framework incorporates the innovation and the skill to assemble information, comprehend it, and institutionalise estimations.



Decision
Should we build this EDW from scratch, or partner with a vendor to deliver this capability for the organization. Are those my only options?

"Do we have the tools to ıse data to transform care delivery and streamline operations?"

"Assessment of our current state indicates we need a different future state. What should that look like?"

"Key to our future state will be an Enterprise Data Warehouse (EDW) to integrate data from multiple sources and facilitate Triple Aim reporting. Make it so."

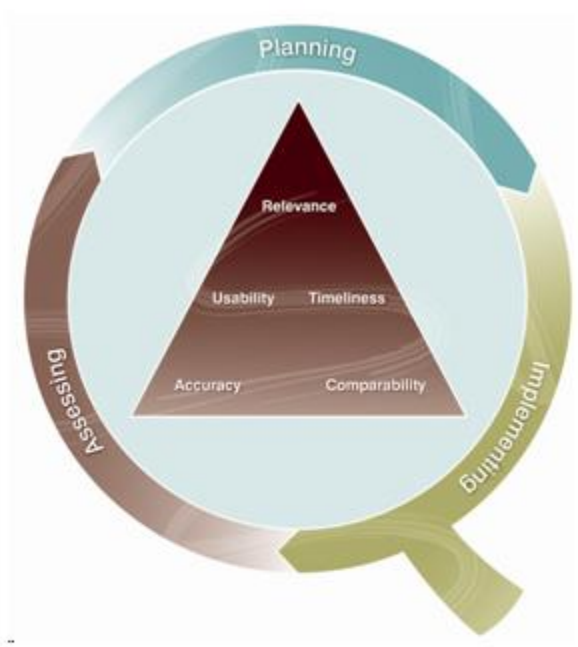
"We will test our EDW to ensure it is meeting our expectations."

"We will roll out our EDW and analytic applications to a broad group of users, including clinicians, leaders, and administrators."

Conglomerating clinical, money related, persistent fulfilment, and other information into Enterprise data warehouse (EDW) is the foundational bit of this framework.

The Content Framework

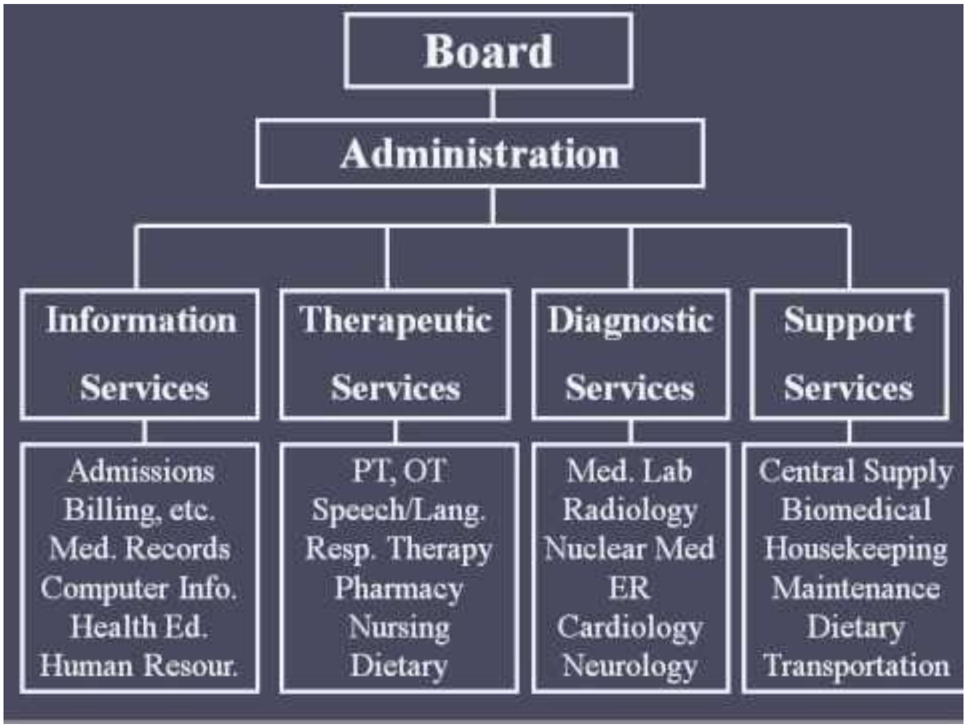
The content framework includes institutionalising learning work—efficiently applying confirmation based best practices to give a second thought conveyance. Scientists make huge discoveries every year about clinical best practices, however, it takes years for these discoveries to be consolidated into clinical practice.



An in number substance framework empowers associations to put the most recent restorative proof into practice rapidly.

The Organisation Framework

This framework includes driving change management through new standard structures. Specifically, it includes actualising group structures that will empower steady, venture wide arrangement of best practices. This framework is in no way, shape or form simple to execute. It obliges genuine authoritative change to drive reception of best practices all through an association.



Therefore, it is explained in the report that an information authorisation and removal activity does not include each of the three of these frameworks; there are chances that it will remain a simply scholastic activity and never leave the research centre of distributed papers. Actualising each of the three empowers a medicinal services association to practically apply information mining to ordinary clinical practice.

2.13 The authentication of data usage application in Healthcare

It has been argued that at the point when these standards are set up, it is seen that have seen that healthcare organisation gain some extremely empowering ground. When organisations actualise the examination establishment to mine the information and organisations have the substance and standard frameworks set up to make information authorisation bits of knowledge significant, organisations are currently prepared to utilise prescient investigation in new and inventive ways.

One of the consumers in the information security framework is a healthcare organisation attempting to succeed in risk based contracts while as yet performing great under the charge for-administration repayment model. The move to esteem based acquiring is a moderate one. Until the flip is exchanged the distance, healthcare system need to outline forms that empower them to straddle both models. This customer is utilising information mining to bring down its evaluation for patients under danger contracts, while in the meantime keeping its patient volume enduring for patients excluded in these agreements. At that point, the health care framework creates procedures to verify these patients get the suitable consideration at the opportune spot and at the correct time.

It is observed that this would incorporate administer to high-chance patients. a danger model (taking into account comorbidity, seriousness score, doctor scoring, and different components) to patients in the registration, run the information through relapse investigation, and appoint a danger score to every patient. The health care framework utilises this score to educate which mind way patients take after release with the goal that organisations get the suitable subsequent consideration.

In spite of the fact that these prescient models oblige a conferred cross-functional group (doctors, technologists, and other workers working in healthcare organisation.) and should be tried over the long run, these customers are content with the advancement and preparatory results. Organisations are moving past the hypothesis of information mining into genuine, realistic utilisation of this method as it is explained in the report of (Stahl, 67-76).

2.14 Data Mining to Improve Primary Care Reporting

The principal activity mines verifiable EDW information to empower Primary Care Provider (PCPs) to meet populace health regulatory measures. This clinic’s PCPs must exhibit to administrative bodies that organisations are giving the proper screenings and treatment to specific populaces of patients. Their centre to date has been on A1’c screenings, mammograms for women more than 40, and influenza shots. The EDW and investigation applications have empowered the PCPs to track their agreeability rate and to take measures to guarantee patients get required screenings.

The Health Catalyst Advanced Application for Primary Care shows slanting of consistence rates and particular estimations over the long haul. In this way, the centre can see how a persisting’s A1’c or LDL results are slanting. Organisations additionally see patients who may at present be in a sound range yet in the course of the most recent 18 months are drifting closer and more like an undesirable result, than proactively address the issue.

Furthermore, the clinic practice in healthcare sectors includes a Nurse Practitioner who joined the practice 20 years prior with a fantasy of changing the standard of nurture diabetes. She attempted to make succinct reports yet pursued into one detour another lastly turned to spread sheets mapped to EMR handle as a reporting instrument, understanding it is a not as much as perfect stopgap. At last, following 20 years, her fantasy materialised with the Health Catalyst answer for convey month to month reports to individual doctors demonstrating their diabetic patients and particular consistence to the standard of consideration. Having this information framework close by has likewise empowered the centre to streamline its patient consideration procedure empowering front-work area staff and medical attendants to handle screening procedures right on time in a patient visit (which gives the doctor more opportunity to concentrate on intense concerns amid the visit). This methodology permits doctors to see more patients and commit more opportunity to those patients' prompt concerns. It permits every individual from staff to work at the highest point of his or her permit and preparing.

2.15 Data Mining to Predict Patient Population Risk

The second activity includes applying prescient calculations to EDW information to anticipate chance inside of specific populaces. This procedure of stratifying patients into high-, medium-, or generally safe gatherings is vital to the achievement of any populace health care administration activity. A few patients convey so much risk that it would be less expensive to pre-emptively send a doctor out to make a house call as opposed to sitting tight for that patient to come in for an emergency arrangement or crisis room visit. The centre should have been ready to recognise these high-chance patients early and centre the fitting assets on their consideration.

To implement better risk stratify the patient populaces; healthcare organisations implement a modern prescient calculation to the information. Utilising the information, it distinguished the clinical and demographic parameters well on the way to foresee a watch over that particular populace. And by applying such a customised calculation to the information, the centre has possessed the capacity to pinpoint which patients require the most consideration well in front of the emergency. Significantly, the facility has coordinated this knowledge into its work process with a straightforward positioning of need patients. This took into account improvement of enhanced procedures for dealing with the consideration of at-risk patients. Case in point, every week the doctors and consideration facilitators examine the danger level of every patient with an arrangement booked for that week. Organisations can then make a consideration administration arrange ahead of time to impart to the patient amid the visit.

The clinic additionally evaluates the Patient Activation Measure (PAM) scores and uses that information to focus tolerant engagement and enactment. This prompts shared choice making between the PCP and the patient, as the doctor has the capacity focus early those patients who are at higher danger for resistance or may be not able to completely take part in their consideration as it is comprehended.

2.16 IT Security Design:

Physical Infrastructure of IT security design

Data centre and disaster recovery

Because of the working pattern in the healthcare sector, medicinal services associations - particularly healing centres - must keep up a high level of framework and system accessibility. Patients' *lives may rely on upon frameworks being up and running, and patients'* health care could be endangered by absence of access to health awareness information in the occasion of framework downtime.

Healthcare sector crushed by tornadoes in Joplin, healthcare organisation discovered that catastrophe recuperation arranging must consider the effect to clinical work processes, particularly in the case of a patient surge. As doctors and clinicians turn out to be more dependent on clinical applications to convey patient care, the significance of calamity readiness and framework strength in social insurance get to be evident.

Tragically, when setting up IT spending plans, numerous health awareness associations ignores the significance of building up a successful calamity recuperation arrangement. It's vital for social insurance CIOs to present the business defence and get a financial plan for fiasco recuperation arranging.

Data backup policy

It is seen that a government Health Insurance Portability and Accountability Act secured substance must have an alternate course of action set up to guarantee proceeded with access to electronic ensured health care data in the case of a framework disappointment. HIPAA catastrophe recuperation necessities additionally incorporate the requirement for an ePHI information reinforcement arrangement, alongside debacle recuperation and crisis mode operation arranges.

Associations adding to a HIPAA catastrophe recuperation arrangement should likewise clarify how delicate social insurance information will be moved without damaging HIPAA protection and security necessities.

Logical framework of IT

The interconnection of layers portrayed above can happen in an assortment of ways utilising blend of layer 2 and layer 3 advancements. Biomedical gadgets, clinical applications and related security prerequisites impact the layer 2 and layer 3 plans.

Centre LAYER

- Serves as the foundation of the system
- A moderate outline setup is received for centre layer to decrease many-sided quality.
- For high accessibility in Hierarchical systems , squares are interconnected

Dispersion LAYER

- Serves as administrations and control limit in the middle of access and centre layers
- Goes about as intelligent confinement point in the occasion of disappointment in access layer
- Burden adjusting, QoS, simplicity of provisioning are key contemplations in this layer.

ACCESS LAYER

- First and foremost purpose of passage into the system for edge administrations, for example, therapeutic gadgets, convenient PCs, end stations and others
- Gives boundary between figuring gadgets and system framework
- It gives QoS, security and approach trust limit and is a key component in empowering different administrations

Security Design

IT execution in Health Care industry has started to change the Healthcare segment totally with current innovation progressions rolled out to improvement the part all together. Electronic Medical records and record trades have enhanced to wind up more secured and dependable. Therapeutic Institution have turn out to be more responsible for the understanding information and records.IT foundation models in Healthcare likewise comprises of remote patient observing, remote prescription counselling or telemedicine, henceforth obliging high system accessibility and additionally security. Access through cell phones to the secured medicinal records of the patients and alternate business application expand the seriousness of the prerequisite of a secured model. Security Issues confronted in Healthcare IT infra-structure can be extensively named:

Ownership of information

Feeling of proprietorship is obliged towards the patient`s restorative data to keep any unapproved access to the information identified with the patients. The group, association or the individual who made the patient information is capable to keep up and secure the information. Information related personals can be partitioned into three classes: Creator, Author, and

Manager. The individual dependable to create the information is alluded as the maker of the information. In the event that EMR Laboratory staffs can be considered as the makers. Creator of information can be alluded to as the clinician. Director to the EMR is the patient self. In some cases there could be some outsider included at this specific level. Security of proprietorship could be performed utilising encryption or watermarking procedures.

Validation of information

Validation of information is obliged to state that specific information set is genuine and lapse free. Endpoint Authentication is seen in the majority of the system construction modelling. It keeps any type of man in the centre assault. A few conventions are utilised to have secured web scanning, sends and faxing, VOIP

Non- denial

It goes about as the electronic mark to accept the exchange. It keeps any foreswearing between gatherings after the finishing of any specific exchange.

Approval and Confidentiality of information

Patient can permit or deny the sharing and use of information for any reason other than his finding. So the ascribes to get to the information is looked after appropriately. Classified of information is characterised by ISO-17799 guaranteeing the entrance just to the individuals why should approve access the information.

Accessibility of information

For EHR to work at the ideal must have high accessibility. So all the frameworks related to upkeep and the utilisation of EHR ought to be accessible 24*7 keeping any kind of administration disturbance. Security and Privacy assurance and HIPPA agreeability help us to accomplish the prerequisite

However, it is important for an organisation to implement professional working system in their working system in order to maintain the balance of their information security. Moreover, the most stable and popular information security pattern in the marketplace are DMZ, Port Security and others.

DMZ

Generally SFTP Servers have been introduced in the DMZ (or open confronting) section of the system since associations were dreadful of opening inbound ports into the Private (interior) system. Keeping the SFTP Server in the DMZ has represented a few issues. The essential issue is that records must be put away in the DMZ when they are dropped off by accomplices, or generally arranged briefly for pickup. Those arranged documents have a higher risk of being gotten to by programmers or hacker since the DMZ is more presented to the Internet. It is oblige those organized documents to be encoded with something like Open PGP, however numerous examiners do not care to see any delicate records in the DMZ, scrambled or not. Another issue is that the healthcare organisation frequently needs to compose scripts to duplicate the documents forward and backward between the DMZ and private system, which requires software engineer exertion and can prompt mistakes.

To keep delicate records out of the DMZ, a few associations have moved their SFTP server into the private system. This methodology wipes out the need to compose scripts for moving records forward and backward. The huge defeat of this methodology is that ports were generally opened into the private system for exchanging accomplices to get entrance to the SFTP server. These open ports could make a potential danger for assailants to get entrance to the private system. In today's security-cognizant environment, most IT reviewers do not care to see any inbound ports opened into the private system, particularly if the workers are putting away delicate PCI or HIPAA information on those servers.

A methodology that is rapidly picking up in ubiquity is to execute a portal segment in the DMZ. The door will serve as an upgraded converse intermediary which does not oblige inbound ports into the private system. At start-up time, the SFTP server will build up an uncommon control channel with the door, which is kept alive consistently. At the point when accomplices join with the passage, it will make demands over the current control channel to the SFTP server. The SFTP server will then open any information channels required back through the portal to benefit the exchanging accomplices. The entire procedure is straightforward to the exchanging accomplices. No information is ever put away in the DMZ since it is basically spilled through the door.

A passage in the DMZ in this manner tackles two noteworthy security issues:

No documents should be put away in the DMZ, including client certifications

No inbound ports should be opened into the Private system

Since a restrictive control channel is utilized to convey between the portal and the SFTP server, it should buy both parts from a solitary merchant. At the point when searching for the right passage for the association, make beyond any doubt it is anything but difficult to situated up and oversee. It is basic that it does not oblige inbound ports into the private system or require any information to be put away in the DMZ.

2.17 Observing of the complete framework

This segment gives a diagram of a construction modelling that helps meet security prerequisites connected with securing clinical frameworks and gadgets, biomedical gadgets/servers, IT endpoints, and their related applications.

ENDPOINT SECURITY

Like in some other industry, social insurance has exceptionally different and complex arrangement of endpoints. Human services suppliers utilise a plenty of both wired and remote gadgets for clinical IT needs. These gadgets should be secure from information misfortune, information burglary, and protection attack, and must additionally meet the nearby nation and state security law. A few Products that can help with end point security are Host Intrusion Prevention programming, Wireless LAN Controller (WLC), Antivirus programming and Trojan-product evacuation devices.

- Securing end focuses satisfactorily taking after things must be finished:
- Authorise security arrangements for clients and gadgets.
- Distinguish and confine clients and gadgets that disregard strategies.
- Oversee characters and control clients on particular gadgets.
- Examine gadget health care, and isolate and remediate gadgets with security issues

System SECURITY

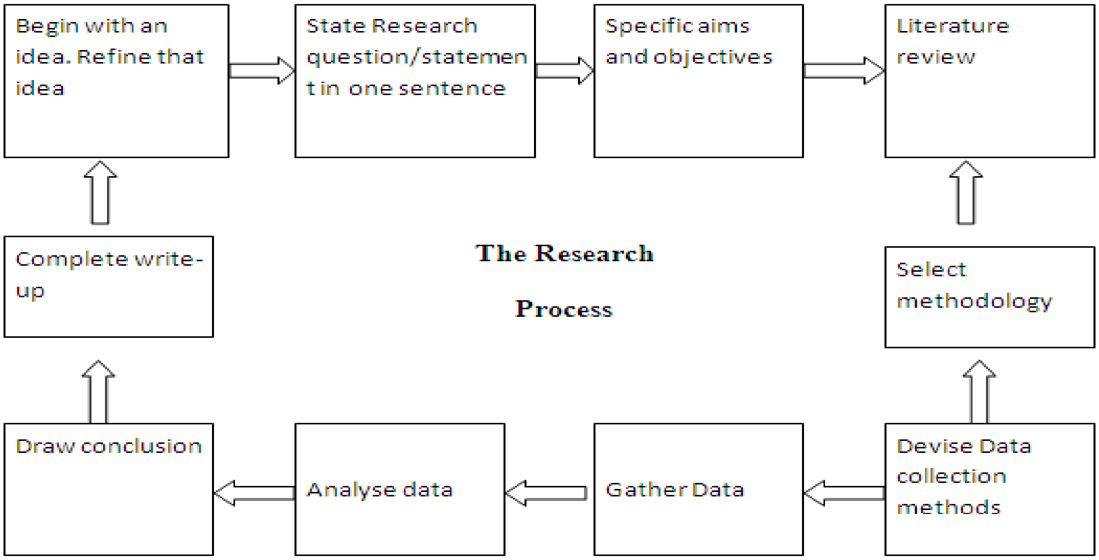
A standout amongst the most central components of the Medical systems is system security, which is intended to ensure the trustworthiness of the system framework itself, where whole system portions may be the objective of assaults, for example, robbery of administration, administration misuse, foreswearing of administration (DoS), and information misfortune. Firewalls must be utilised to isolated the system and anticipate unapproved access. Moreover, Network security can be improved by utilising Security Appliances gave by sellers, for example, Cisco. VPN must be utilised for getting to the Medical system from outside. Switches likewise must be furnished with firewalls. Framework assurance must be given on Routing/Switching stages

This segment gives a diagram of a construction modelling that helps meet security necessities connected with securing clinical frameworks and gadgets, biomedical gadgets/servers, IT endpoints, and their related applications.

CHAPTER 3 METHODOLOGY

3.1 Introduction

The chapter of research methodology accentuates and focuses upon the ways through the help and application of which the research will be carried. It helps to understand the research format through which it is being conducted and the necessary steps that have been taken for the effective conduction of the research on the whole. Figure below is a research process model and it shows proposed steps from beginning to end of a research process:


Begin with an idea. Refine that idea
State Research question/statemen t in one sentence
Specific aims and objectives
Literature review
Complete write-up
The Research Process
Select methodology
Draw conclusion
Analyse data
Gather Data
Devise Data collection methods

3.2 Research Method

The method to carry out this study is qualitative. The qualitative research method fundamentally provides a deep understanding of the analysed phenomenon. Qualitative research is defined as an activity to acquire knowledge about the cultural and social realities defined in specific contexts) (Merriam, 67-77).

3.3 Justification and Recommendation of Approach

This research will follow a deductive approach and will be and cross-sectional in nature being a study of particular phenomenon at a particular time. The rational for this approach is that deductive approach starts from the unknown to be applied to the known general to specific, from the abstract (or principles) to be applied to the concrete .Using this approach researcher will be able to discover new dynamics and significance of safe management of electronic health data in Saudi Arab (Silverman, 164-152).

3.4 Data Collection

A data collection method can be defined as a tool to collect data in the field. There are two types of data utilised in the qualitative academic inquiries; primary data and secondary data. This study will utilise the primary data. There are three tools to collect the data a study. These are: participant observation, interview and questionnaire survey (Merriam, 174-178). This study will collected primary data through a survey.

3.4.1 Survey

This study seeks to conduct a survey of the employees of King Fahad University hospital to measure their perceptive on healthcare data and information security framework in the hospital. The survey is a technique of field research; for greater information gathering, the survey is often used as an alternative to the constraints presented by observation (Maxwell, 167-178).

3.4.2 Questionnaire

In order to conduct a survey of healthcare sector in different Saudi Arabian hospitals for the assessment of healthcare data and information security framework an exclusive questionnaire as a data collection instrument will be designed. The research questionnaire will divided in to various sections to obtain perspective of participant on the assessment of healthcare data and information security framework in three particular three areas i.e. end-user (employees, doctor and Nurses), IT security team and IT design.

3.4.3 Population and Sampling

The term population refers to a set of individuals, organisations, event or object that the researcher intends to study. The population in this proposed research will be customers of Tesco based in London, the sample population will be chosen randomly, and the customers will be sent the questionnaires electronically along with a request to participle in this academic inquiry. Researcher will try to contact 150-200 employee of King Fahad Medical City in order to obtain their perspective.

The population in this proposed research will be users of health data and IT staff of hospitals, the sample population will be chosen randomly, and the participants will be sent the questionnaires electronically, along with a request to participle in this academic inquiry. The researcher will aim to contact 150-200 relevant people in order to obtain their perspective, research expect this population size would ensure the vigour of this study.

3.5 Data Analysis

The collected data will be analysed appropriate method and analysed data is presented along with interpretation in the form of figures and graphs

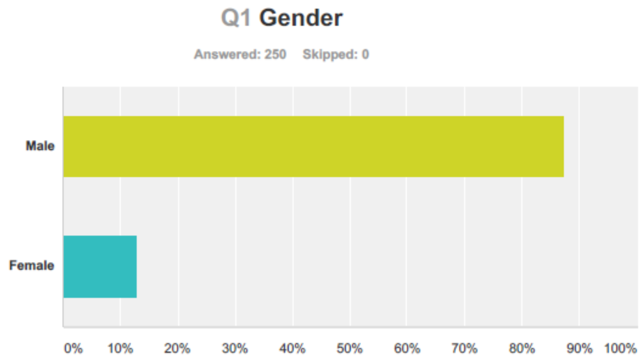
3.6 Ethical Consideration

This study has is looking forward utilised wide range of secondary data, initially to establish the conceptual foundation of research question and secondary to answer this question from the existing body of contemporary literature. The major ethical consideration in this study will be to utilise authentic, creditable, pertinent and current. In order to ensure this facet, research only use peer review articles, official reports and official website.

In the same vein another ethical consideration will be to maintain originality of this research, to ensure this research using Harvard style of referencing has properly cited each and every academic source from where any information is taken for this research. Another major ethical will be in the presentation of primary data, this proposed research following the standard guideline will ensure the anonymity of all participants of survey and their personal information, name, designation, and others will not be revealed in this research.

CHAPTER 4 RESULT AND DISCUSSION

4.1 Results



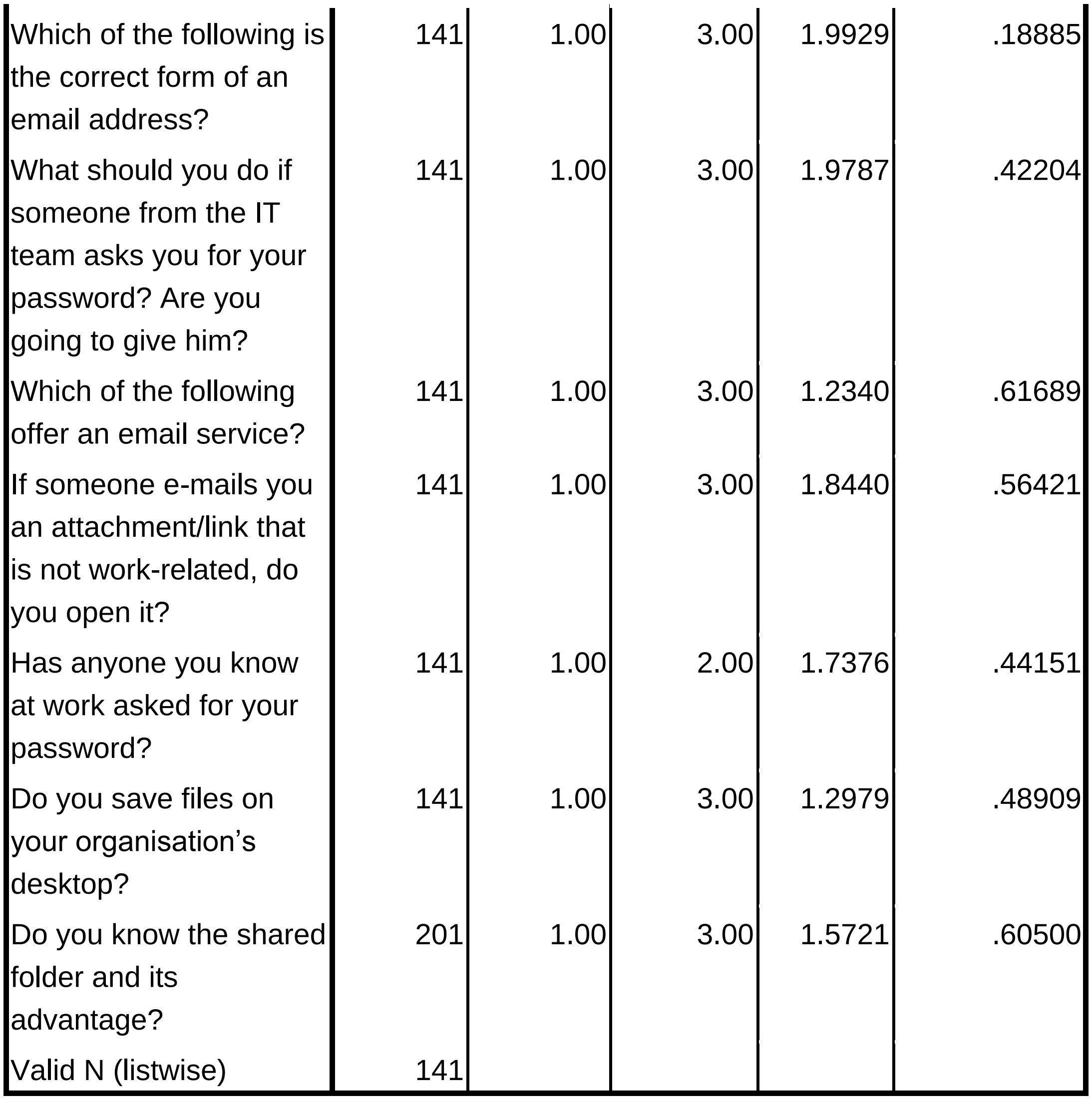
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Gender?	250	1.00	2.00	1.1280	.33476
Valid N (listwise)	250				

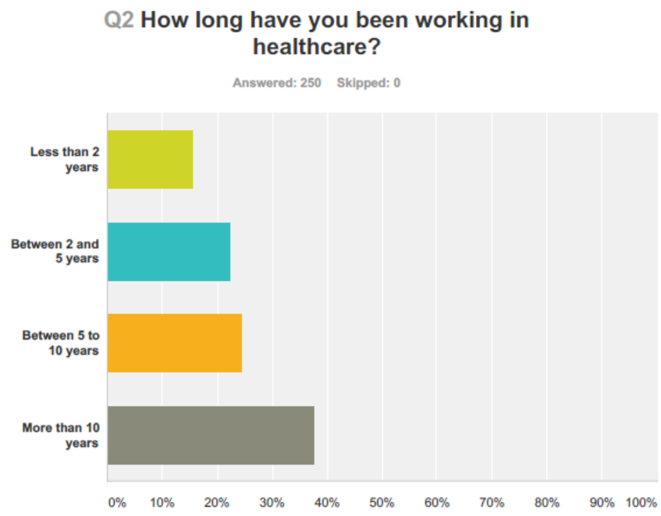
Most of the participant responded to the questionnaire survey on SurveyMonkey are found male with approximately 86% however, only 11% of the respondents were female.

Descriptive Statistics

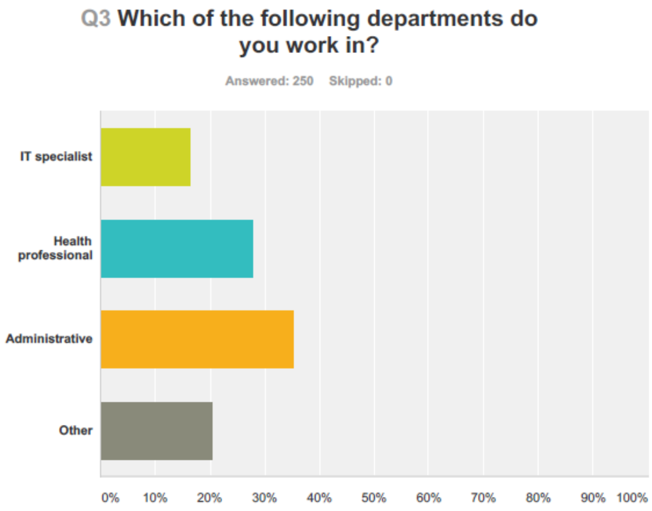
	N	Minimum	Maximum	Mean	Std. Deviation
How long have you been working in healthcare?	250	1.00	4.00	2.8400	1.09691
Which of the following departments do you work in?	250	1.00	4.00	2.5960	.99031
Which one of these examples is the strongest password?	250	1.00	3.00	2.8520	.43687



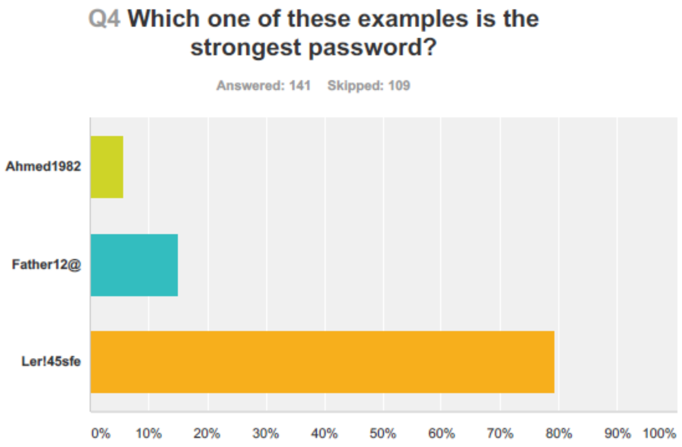
Which of the following is the correct form of an email address?	141	1.00	3.00	1.9929	.18885
What should you do if someone from the IT team asks you for your password? Are you going to give him?	141	1.00	3.00	1.9787	.42204
Which of the following offer an email service?	141	1.00	3.00	1.2340	.61689
If someone e-mails you an attachment/link that is not work-related, do you open it?	141	1.00	3.00	1.8440	.56421
Has anyone you know at work asked for your password?	141	1.00	2.00	1.7376	.44151
Do you save files on your organisation’s desktop?	141	1.00	3.00	1.2979	.48909
Do you know the shared folder and its advantage?	201	1.00	3.00	1.5721	.60500
Valid N (listwise)	141				



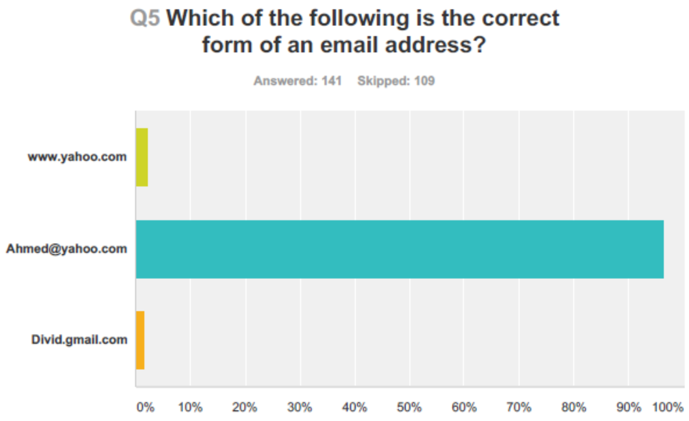
There were many respondent participated in the survey that are engaged with the healthcare sector with more than 10 years. Moreover, there were participants that have recently joined healthcare sector and are proving their services.



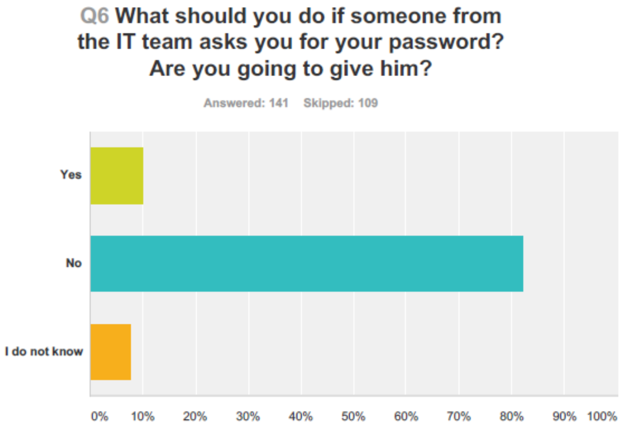
Most of the participants that participated in the survey were engaged with the administrative department of their respective healthcare organisations. Moreover, a number of participants were also involved in healthcare organisation as health professional and IT specialists.



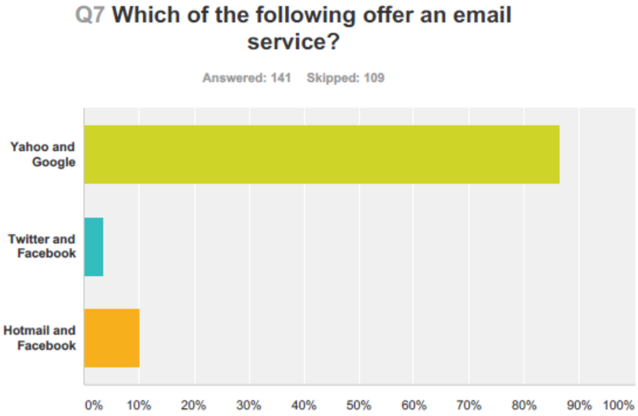
Almost 80% of the survey participants who participated in the survey have complicated passwords for different purposes in order sustain their privacy from other.



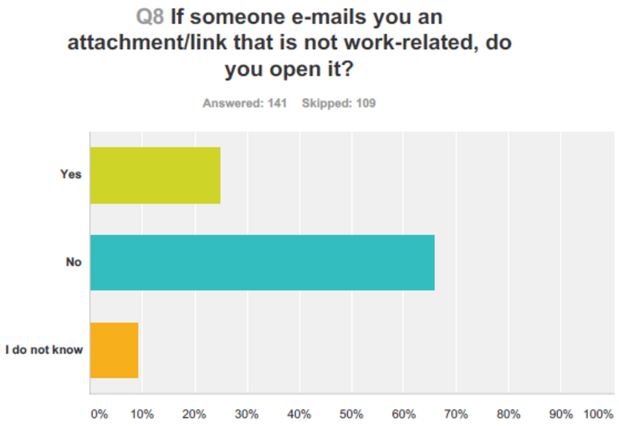
Among all the participant, the most appropriate email for is ahmed@yahoo.com, almost 99% of the participants have agreed to the second option of the question.



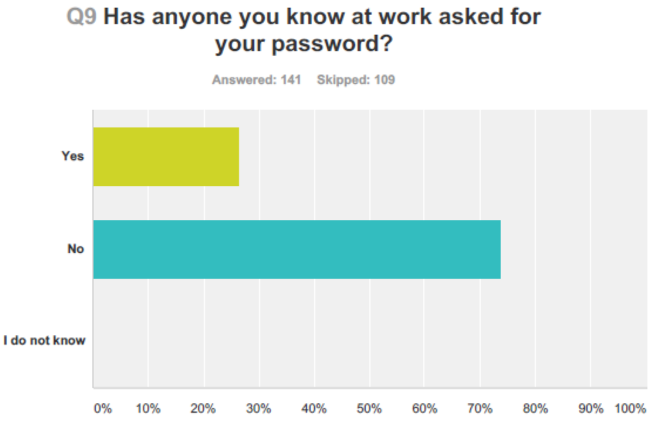
80% of the participants that responded to the questionnaire agreed to the statement that they are not comfortable with sharing their email address with the IT specialist of the organisation.



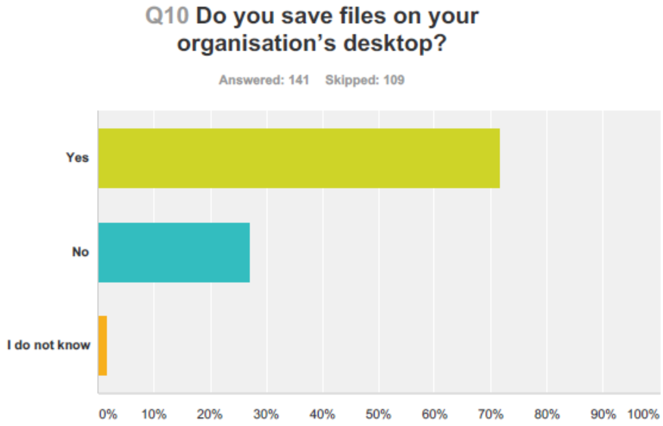
87% of the survey participant agreed to the fact that Yahoo and Google are the services that provide emails to their users.



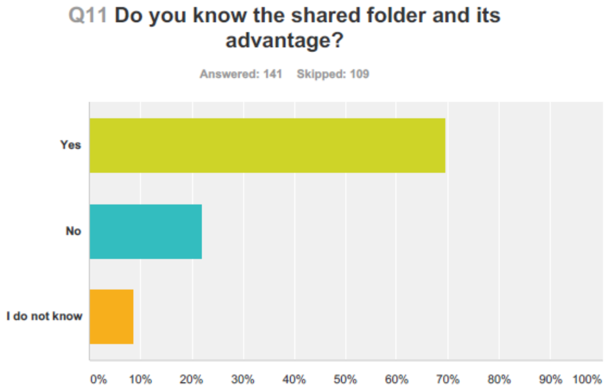
69% of the responded are not interested in opening the attachments that are not related to their work.



Most of the participants agreed that co-workers and colleagues in organisation do not ask for other employee's password as it is found unethical to ask others for their password.



Among more than 70% people that participated in the survey are keen to save their work related files on their desktop as they are convenient with that. However, 29% participants properly save their files at drive location on the organisation's data server.

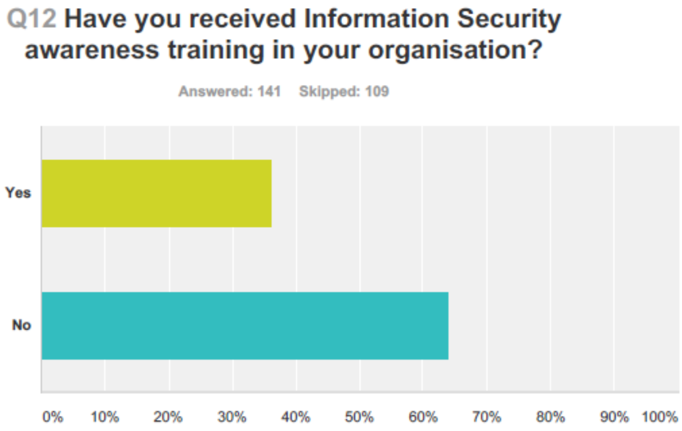


70% of the participants know the advantages and uses of saving files in the share folder however, only 20% participant are unaware of its benefits and uses.

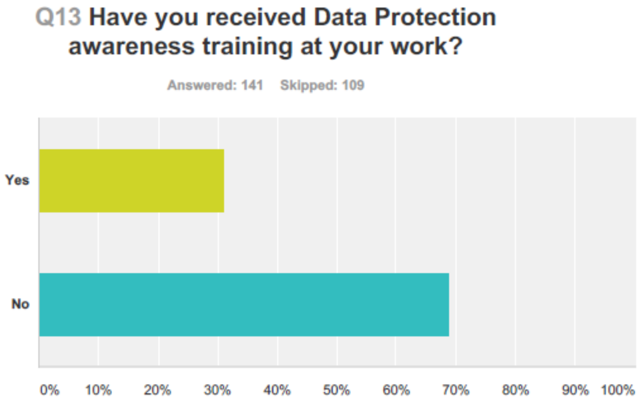
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Do you save files on your organisation's desktop?	141	1.00	3.00	1.2979	.48909

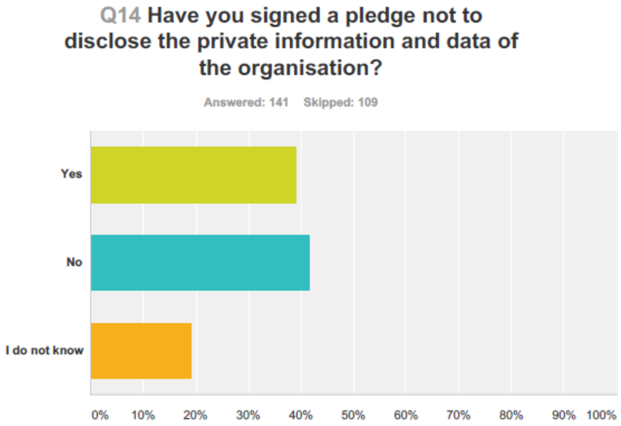
Do you know the shared folder and its advantage?	201	1.00	3.00	1.5721	.60500
Have you received Information Security awareness training in your organisation?	141	1.00	2.00	1.6383	.48221
Have you received Data Protection awareness training at your work?	141	1.00	2.00	1.6879	.46498
Have you signed a pledge not to disclose the private information and data of the organisation?	141	1.00	3.00	1.8014	.73892
What is the state of security awareness training in your organisation?	141	1.00	3.00	1.9787	.84910
Do you think that you need basic security awareness training when you join your organisation?	141	1.00	3.00	1.1702	.47746
Do you think sharing games or programs with your co-workers will impact on the information security in your organisation?	141	1.00	3.00	1.6312	.79652
Do you think that your organisation’s computer is secure?	141	1.00	3.00	1.7021	.76293
Do you know that the Anti- virus software is enabled?	141	1.00	3.00	1.6099	.86827
Valid N (listwise)	141				



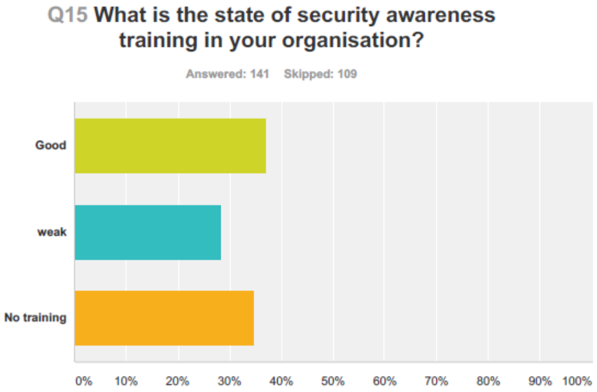
35% of the employees in organisation receive security awareness training programs in their organisation. Moreover, there is still approximately 65% of the participant who has not received any type of society awareness training programs at their respective organisations.



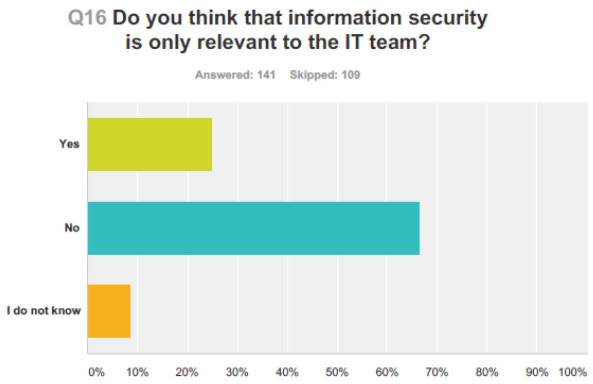
70% of the employees working in different organisational sectors do not receive any type of data recovery training at their work on the contrary about 30% of the respondents were positive regarding the data recovery training at their organisation.



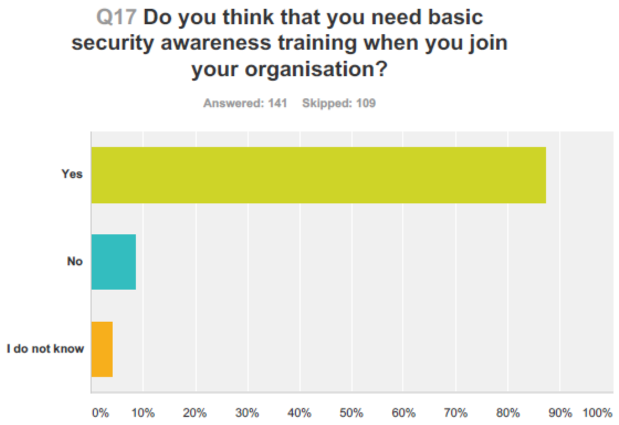
40% of the respondent in the survey have not sign any type of pledge regarding the disclosure of organisational information however, 37% respondent have signed non-disclose agreement with the company regarding sharing the information of the organisation. Among them there were about 20% of the respondent that do not know anything regarding non-disclose agreement with the company.



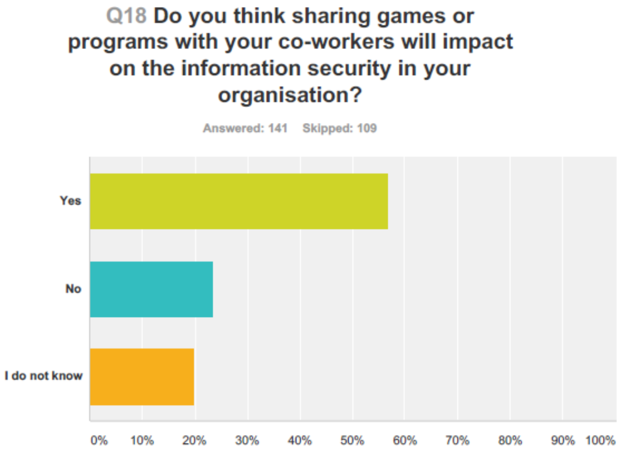
40% of the respondent receive good security awareness training at their organisation however, there are also respondent about 27% that receive only basic training of security awareness training at their organisation.



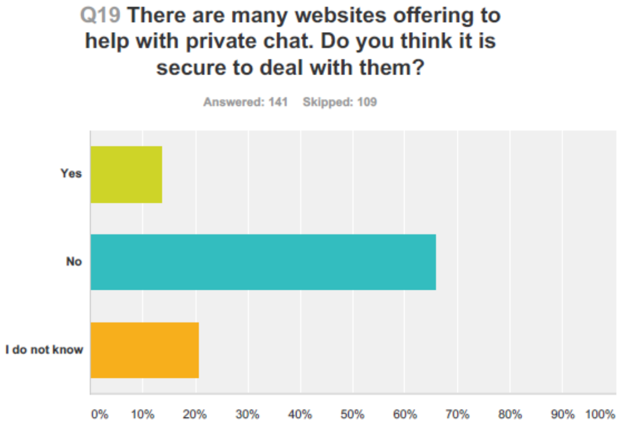
About 70% of the respondent thinks that the information and data security is not linked with the IT team but all the working staff of the organisation.



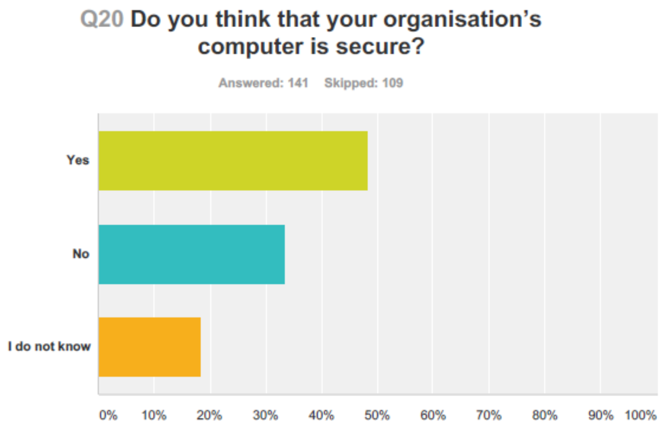
Majority of the respondent thinks that they should receive basic security awareness training with the start of their professional career in organisation.



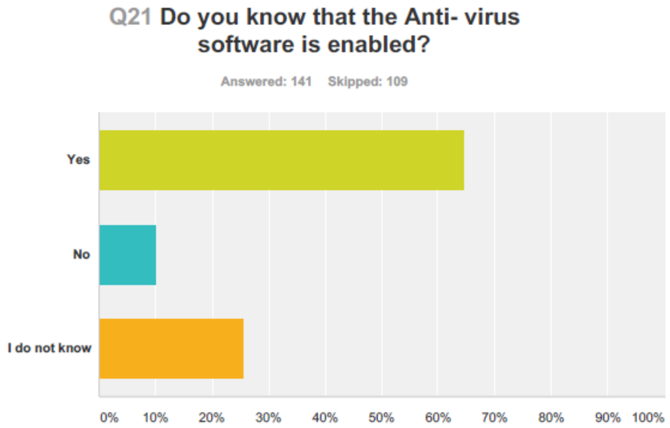
About 60% of the respondents are positive that sharing games and programs with their colleague might affect the information security of their organisation.



More than 60% of the respondent thinks that taking help from other online websites in cracking deals are secure and they do not affect the information data of the organisation however, only 20% respondent thinks that these online websites affect the information of the organisation.



About 50% of the respondent believes that the organisation's computer is secure from external elements on internet.



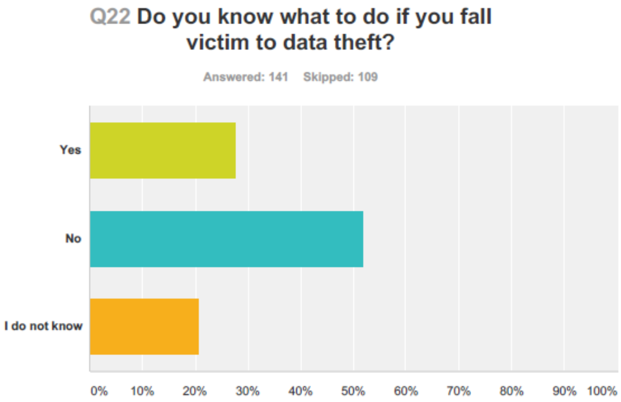
65% of the respondent knows that usually anti-virus is enabled at organisation's computer in order to secure their internal information.

Descriptive Statistics

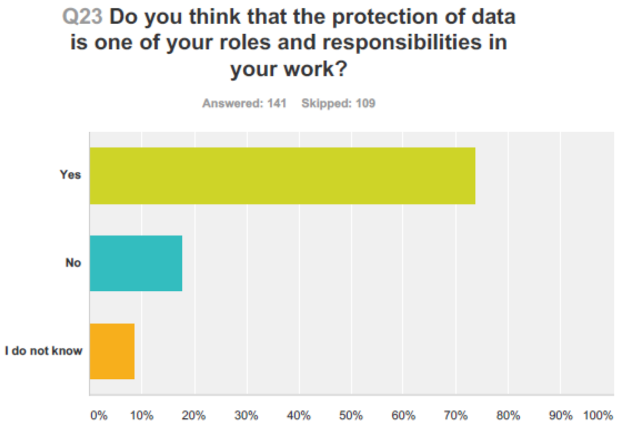
	N	Minimum	Maximum	Mean	Std. Deviation

It is allowed to use your personal computer (laptop or mobile device) to connect to your organisation's network?	33	1.00	3.00	1.6061	.60927
Do you think your computer has no value to hackers, so they do not target you?	33	1.00	3.00	2.1212	.59987
Do you know what a phishing attack is?	33	1.00	2.00	1.3333	.47871
Do you think that the anti-virus software is enough to protect the computers in your organisation?	33	1.00	3.00	2.0909	.57899
Do you think that opening the internet to allow employees in your organisation to download files and videos will affect network security, even if you have strong antivirus software?	33	1.00	3.00	1.3030	.58549
Is it allowed in your organisation to use personal routers (wireless internet devices)?	33	1.00	3.00	1.7576	.56071
Do you think the rouge access point will impact on wireless in your organisation?	33	1.00	3.00	2.1212	.96039
Does your organisation implement DMZ?	33	1.00	3.00	2.1515	.97215

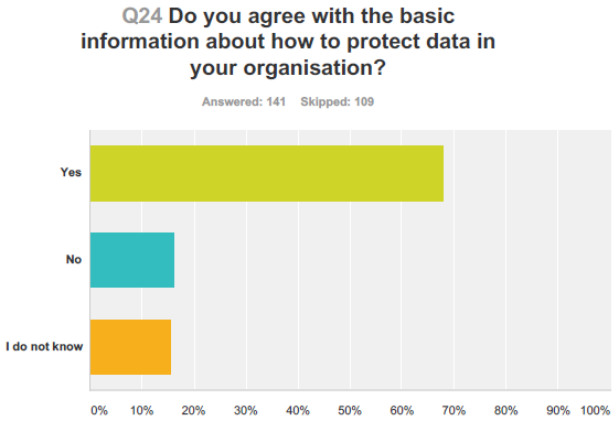
Do you think your organisation is protected and secure?	33	1.00	3.00	1.7879	.78093
Do you think that you are familiar with servers and security devices that are under your responsibility?	33	1.00	2.00	1.3939	.49620
Valid N (listwise)	33				



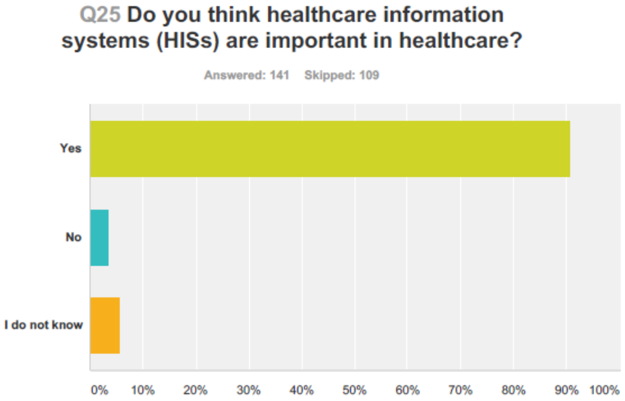
Majority of the respondent are not aware the techniques to cope up if they fall as a victim to data theft.



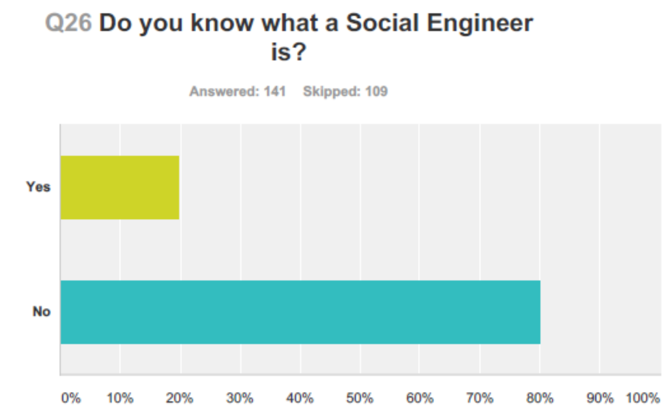
70% of the respondent believes that the protection of data and information of organisation come in their own area of responsibility and roles in their particular organisations.



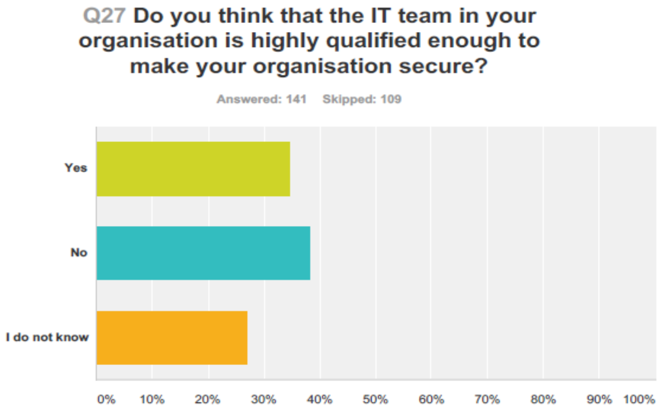
70% of the respondents are aware of the techniques and basic information regarding the security of the internal data and information of their organisation.



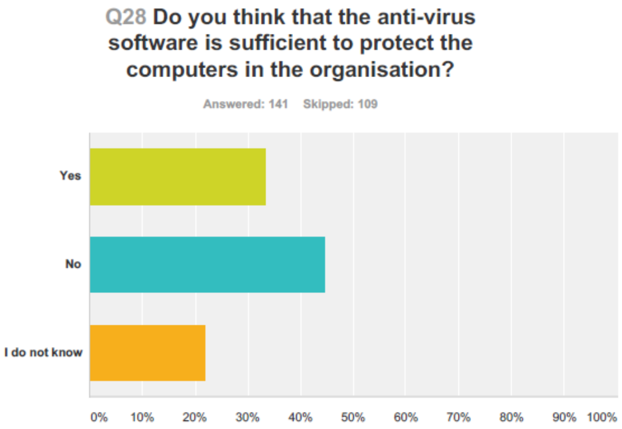
90% of the respondent relies on the fact the healthcare information system plays an important role in the sustainability of information security in healthcare organisation.



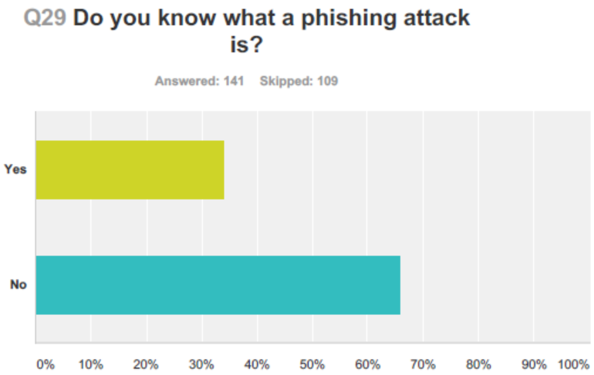
About 80% of the respondent does not know what a social engineer is and what their role is to maintain the data information of organisation.



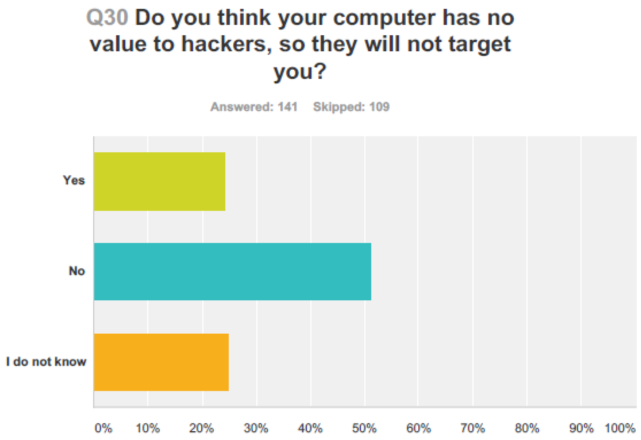
Most of the respondent thinks that they have not enough competent and efficient IT team working at their organisation. However, there are respondent that believe that they have enough competent and effective IT team to protect the data information of the organisation.



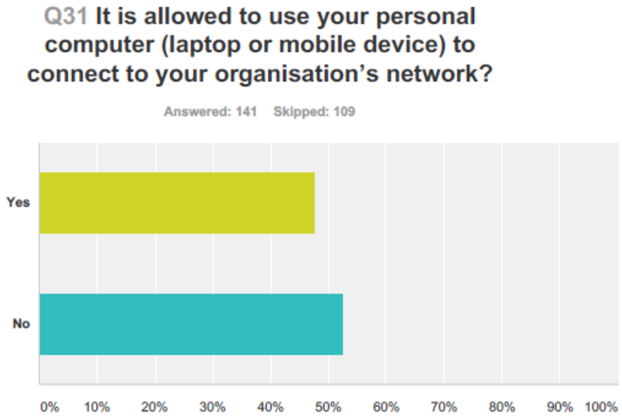
45% of the respondent believes that anti-virus software is not enough to protect the information data of the organisation.



Most the respondent working in different organisation does not know what phishing attack is and how it affects the internal information of the organisation.



50% of the respondent are unaware of the fact the hackers directly attack the main server of the organisation rather than attacking any individual's system or personal computer.



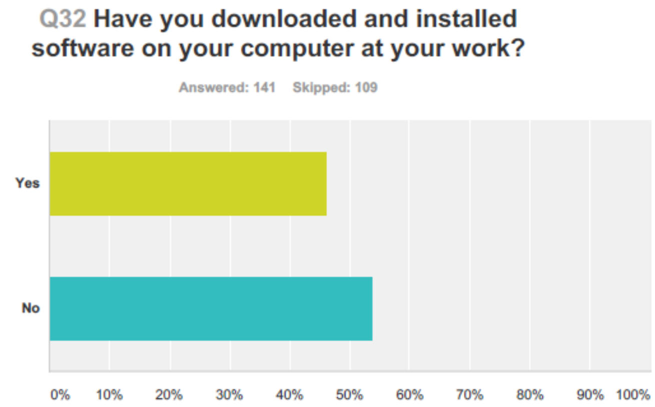
About 50% of the respondent participated in the survey are not allowed to connect their personal pc, mobile and other electronic gadgets to organisation's network. However, about 40% of them are allowed to connect their gadgets with organisation's network.

Descriptive Statistics

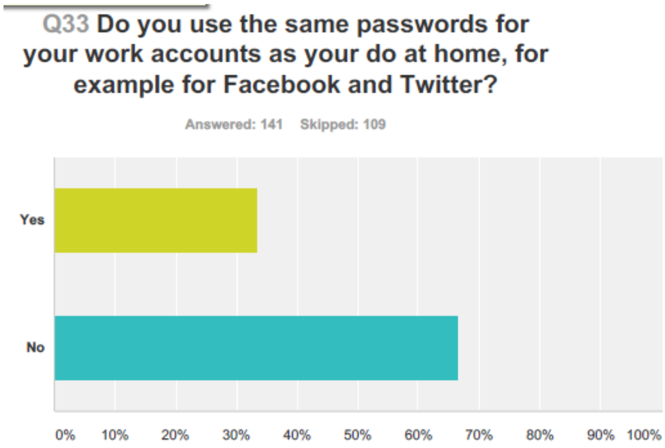
	N	Minimum	Maximum	Mean	Std. Deviation

It is allowed to use your personal computer (laptop or mobile device) to connect to your organisation’s network?	141	1.00	2.00	1.5248	.50116
Have you downloaded and installed software on your computer at your work?	141	1.00	2.00	1.5390	.50025
When you delete a file from your computer, can that file be recovered?	141	1.00	3.00	1.7163	.87281
Do you think you are familiar with all IT devices under your section (computer, Scanner, Fax & printer)?	141	1.00	2.00	1.3121	.46498
Do you think your organisation monitors user activity, and controls access to activity and audit logs?	33	1.00	2.00	1.3333	.47871
Do you analyse network logs in real time, looking for evidence of mounting attacks?	33	1.00	3.00	1.8485	.71244
Do you think your organisation has an incident response and disaster recovery plan and policies?	33	1.00	3.00	1.3636	.54876
Do you think your organisation has a policy controlling mobile and removable computer media?	33	1.00	3.00	1.4848	.66714

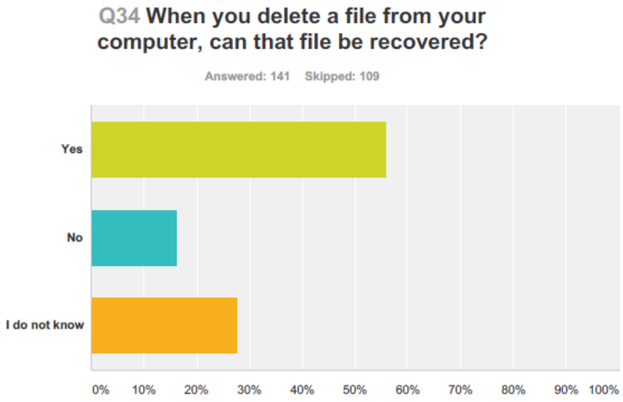
Do you know penetration testing?	33	1.00	2.00	1.4545	.50565
Do you protect networks against internal and external attacks with firewalls and penetration testing?	33	1.00	3.00	1.3636	.69903
Valid N (listwise)	33				



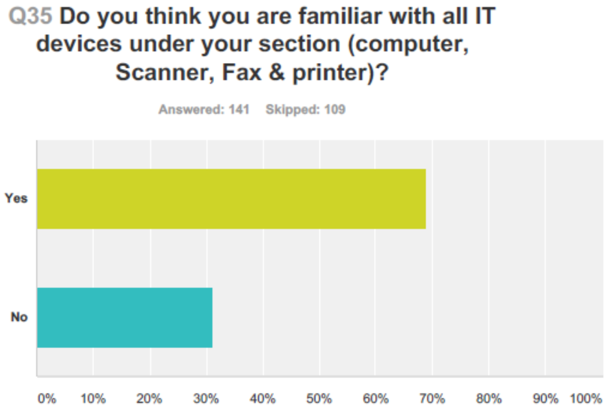
About 55% of the participant have not downloaded or installed software at their organisation's computer as it is not allow in organisation to download anything from their own choice.



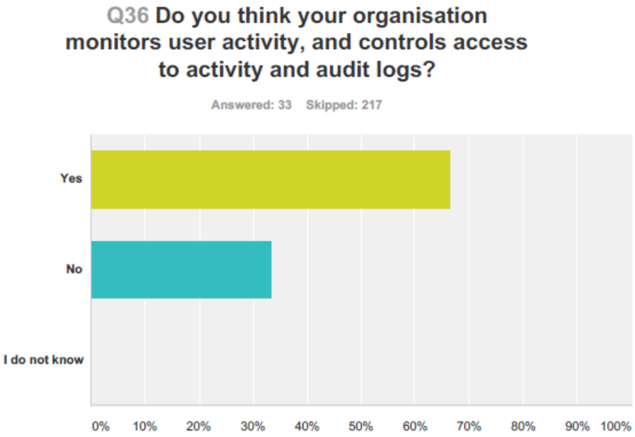
More than 60% of the participants in the survey use different password for their organisational and personal emails like twitter, Facebook, and other.



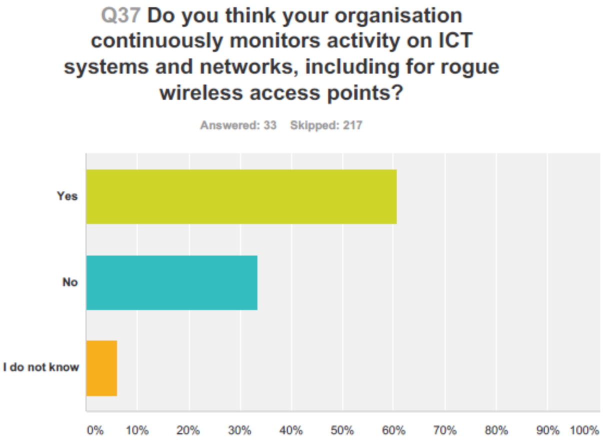
About 50% of the respondent is sure that when they delete any file from their organisational computer, it can be recovered from the main server of the organisation.



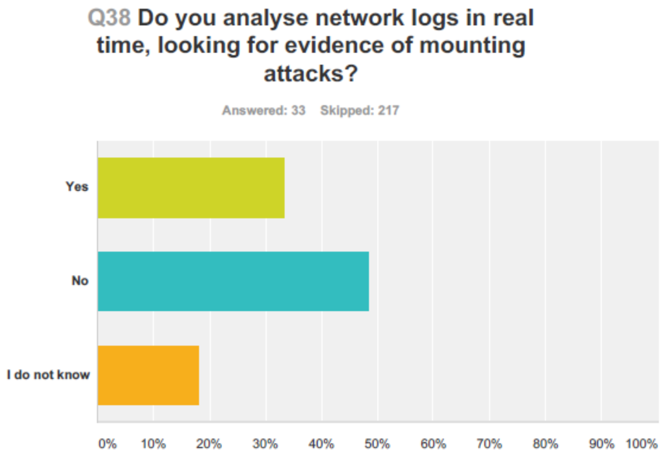
Majority of the respondent are familiar with all IT equipment like fax machine, printer, computer, and other.



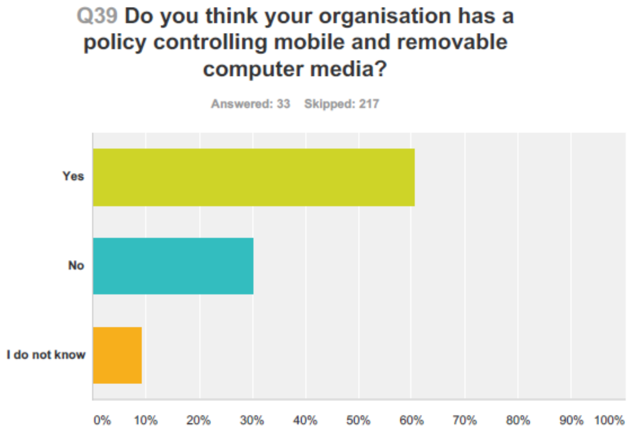
About 70% of the employees are aware that normally organisation and their IT department monitor their employee's activities. Furthermore, they also control employee's usage in regards of their online activities and others.



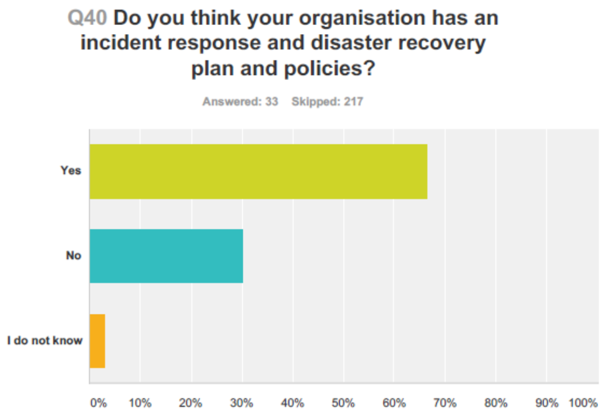
Majority of the survey responded believes that organisation monitor the online activates of their employees that further includes, wireless access points and others.



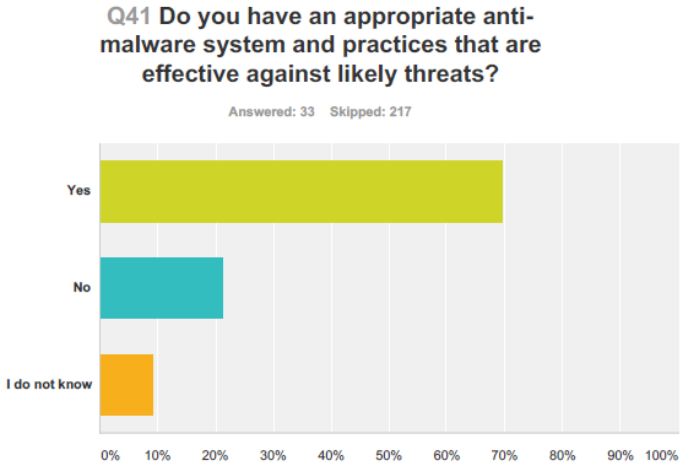
About 50% of the responded are negative regarding the analysis of network logs in regards of looking for evidence of mounting attacks.



About 60% of the survey participants agreed to the fact that their respective organisation has mobile and computer media controlling policy.



More than 60% of the respondents are sure that their organisation has response and disaster recovery plans and policies.

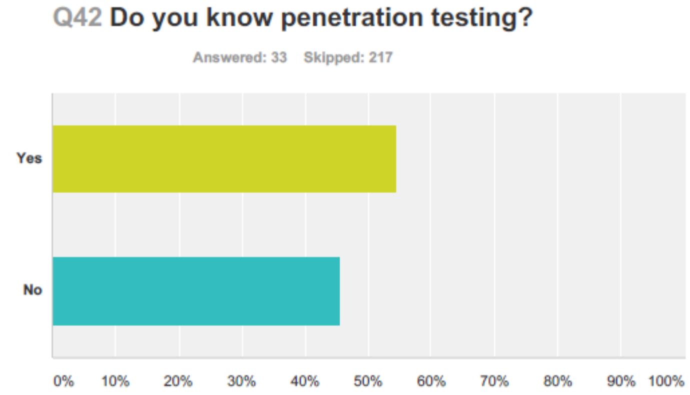


Majority of the respondent have effective anti-malware systems that are effective for all threats regards information security.

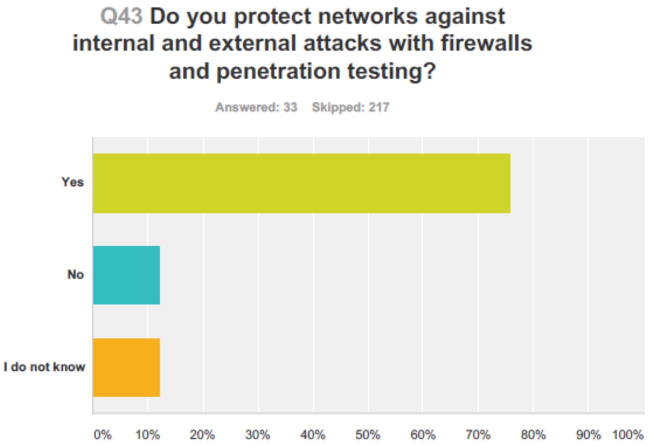
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation

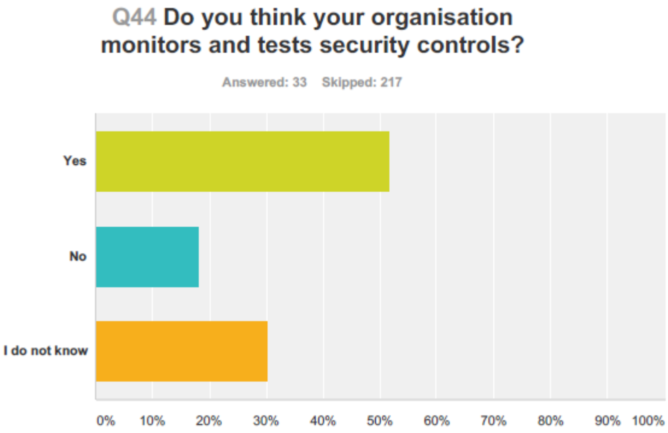
Do you think that you are familiar with servers and security devices that are under your responsibility?	33	1.00	2.00	1.3939	.49620
Does your organisation implement DMZ?	33	1.00	3.00	2.1515	.97215
Does your organisation have a physical backup of the Data Centre (disaster recovery)?	33	1.00	3.00	1.3333	.59512
Are there any records of who accesses the Data Centre (DC)?	33	1.00	3.00	1.4242	.70844
Does the Data Centre have camera monitoring?	33	1.00	3.00	1.2727	.62614
Is the Data Centre (DC) location in your organisation available for anyone from the IT team to access?	33	1.00	3.00	1.6667	.59512
Does your organisation have IDS or IPS systems?	33	1.00	3.00	2.1515	.93946
Do you continuously scan the network and attachments for malware?	33	1.00	2.00	1.3030	.46669
Do you continuously scan for new technical vulnerabilities?	33	1.00	2.00	1.3939	.49620
Valid N (listwise)	33				



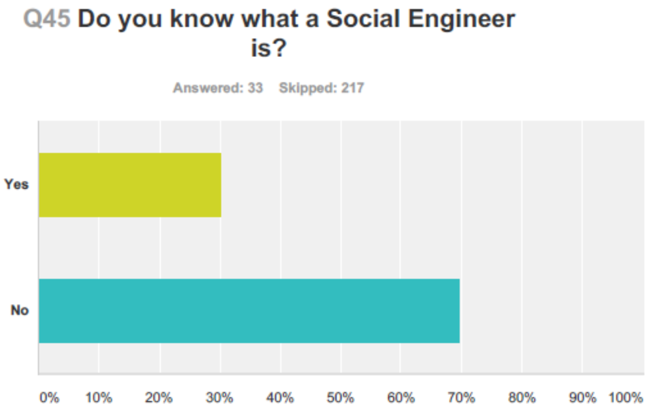
There are mix responds among the respondent that participated in the survey regarding the penetration testing in organisation.



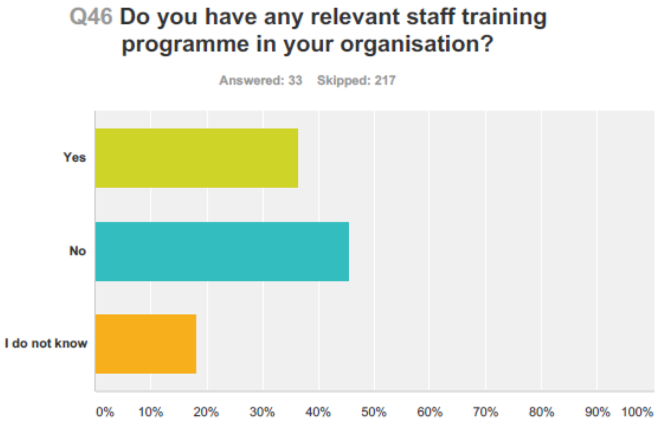
Most of the participant protects their network from internal and external information attack by the help of firewalls and penetration testing.



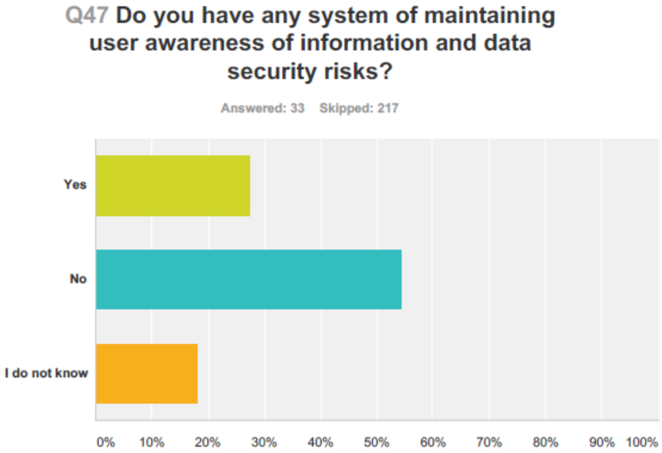
More than 50% of the participants participated in survey are sure that their organisations monitor and test security control in their respective organisation.



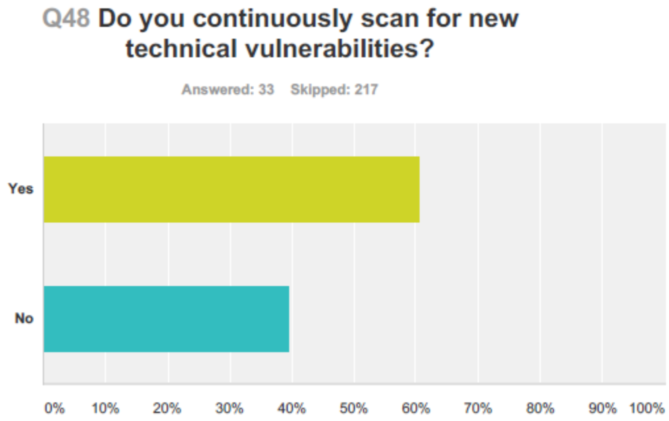
About 80% of the respondent does not know what a social engineer is and what their role is in maintain the data information of organisation.



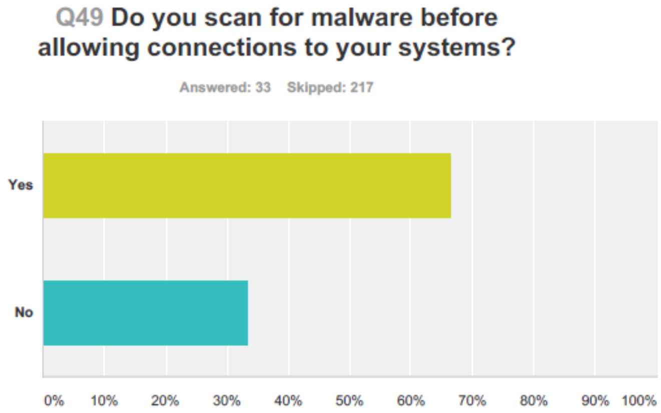
Most of the participant do not have any staff training programmes in their organisation to train them moreover about 30% of the participants have staff training programmes in their respective organisations.



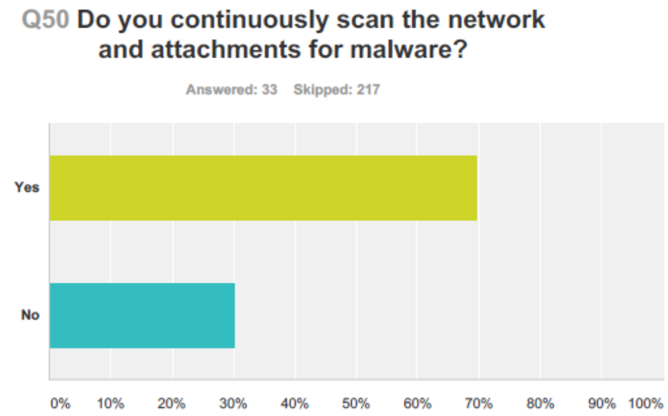
Approximately 60% of the total respondent that participated in the survey does not have any system to maintain user awareness of information and data security risks.



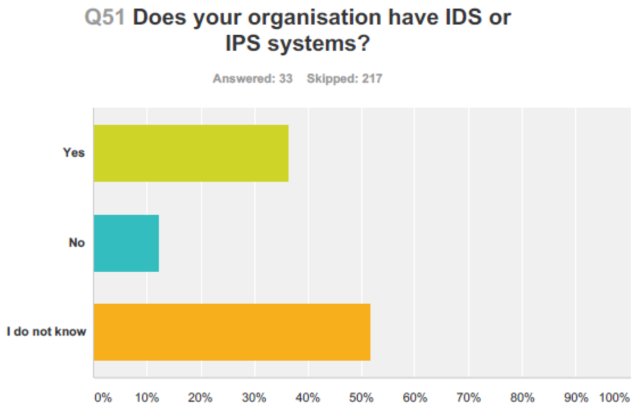
Most of the users that take part in the survey continuously scan their researches for new technical vulnerabilities.



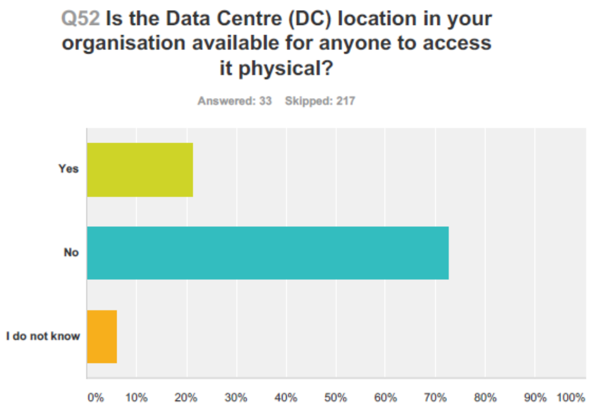
About 70% of the internet and technological friendly participated in the survey scan their system for any malware virus



70% of the participant participated in the survey scan their system network and its attachments for malware viruses.



50% of the survey participants are unaware about the IDS and IPS system of their respective organisation.

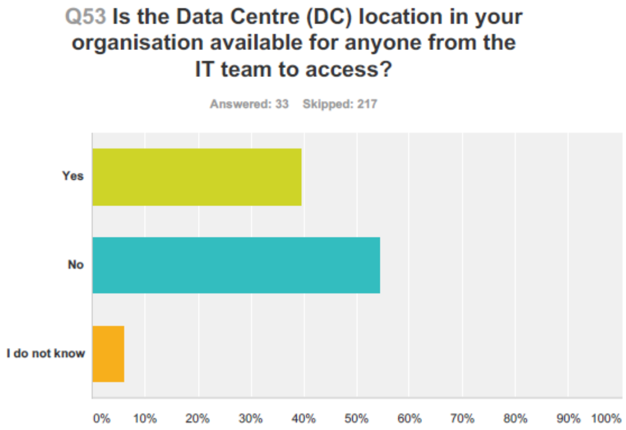


More than 70% of the participants are negative regarding the usage of organisation's Data centre of their organisation for its access.

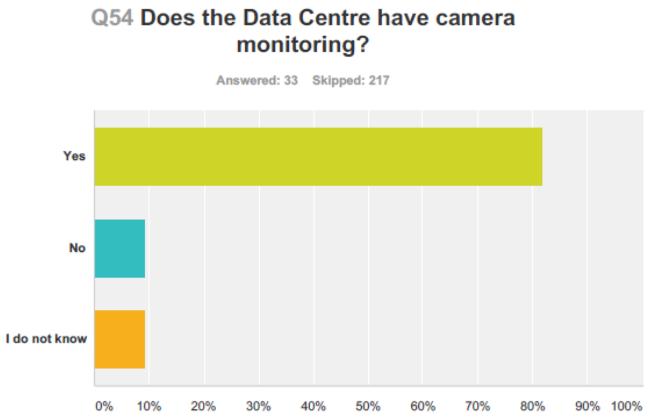
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Do you think your organisation has an incident response and disaster recovery plan and policies?	33	1.00	3.00	1.3636	.54876
Do you have an appropriate antimalware system and practices that are effective against likely threats?	33	1.00	3.00	1.3939	.65857
Do you know penetration testing?	33	1.00	2.00	1.4545	.50565
Do you protect networks against internal and external attacks with firewalls and penetration testing?	33	1.00	3.00	1.3636	.69903

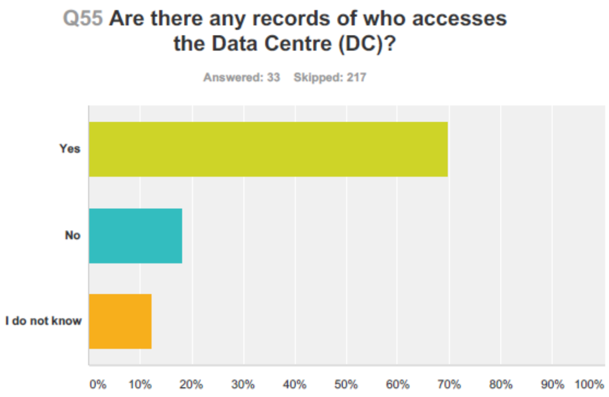
Do you think your organisation has a policy controlling mobile and removable computer media?	33	1.00	3.00	1.4848	.66714
Do you think your organisation continuously monitors activity on ICT systems and networks, including for rogue wireless access points?	33	1.00	3.00	1.4545	.61699
Do you think your organisation monitors user activity, and controls access to activity and audit logs?	33	1.00	2.00	1.3333	.47871
When you delete a file from your computer, can that file be recovered?	141	1.00	3.00	1.7163	.87281
Do you use the same passwords for your work accounts as your do at home, for example for Facebook and Twitter?	141	1.00	2.00	1.6667	.47309
Do you think your computer has no value to hackers, so they will not target you?	141	1.00	3.00	2.0071	.70200
Valid N (listwise)	33				



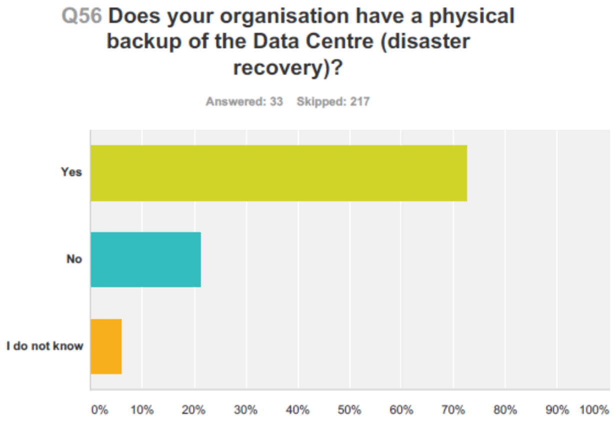
50% of the participants in organisation are positive that even the IT team have not gain the access of data centre of their organisation.



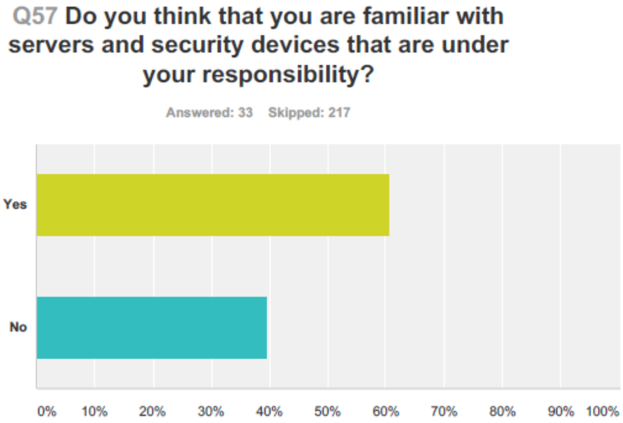
More than 80% of the survey participants have witness camera monitoring at the data centre of their organisation.



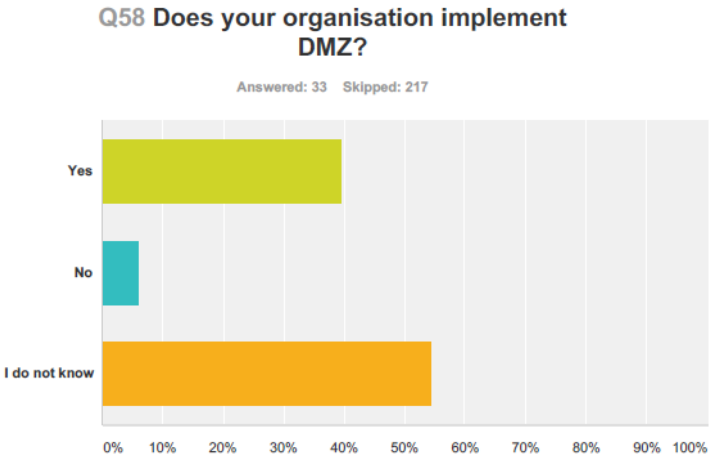
70% of the participants know that organisations have complete records regarding the people who access the data centre of organisation from time to time.



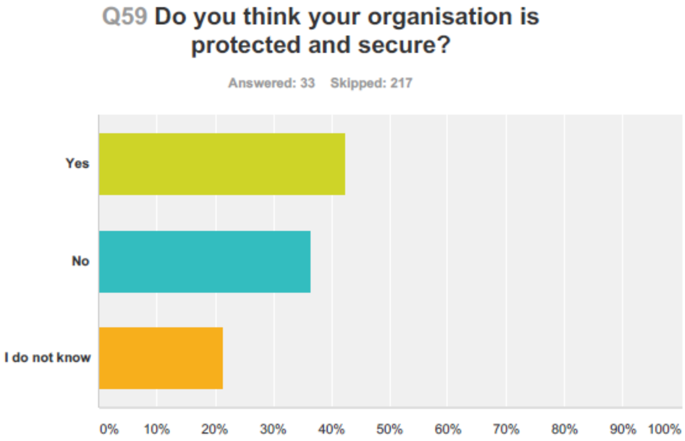
70% of the participants of the survey are positive regarding the physical backup of the data centre of their respective organisation.



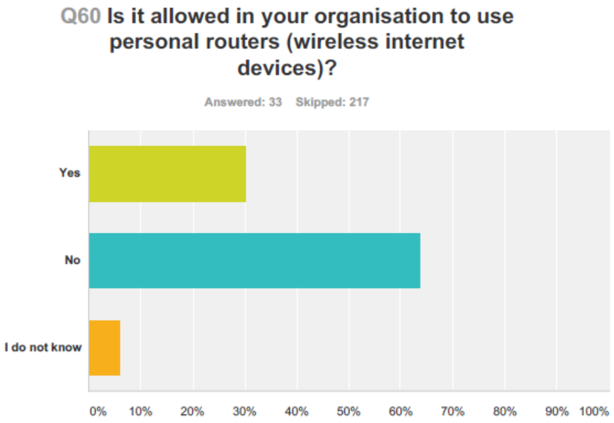
More than 60% of the participants are familiar with the servers and security device that comes under their roles and responsibilities in a particular organisation.



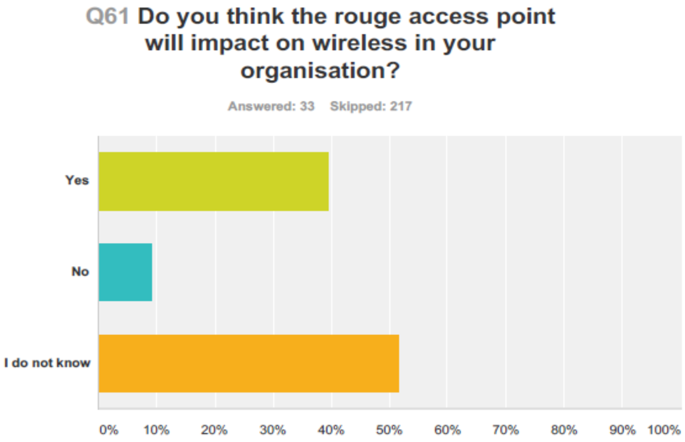
Most of the participants have no knowledge regarding the implementation of DMZ in an organisation.



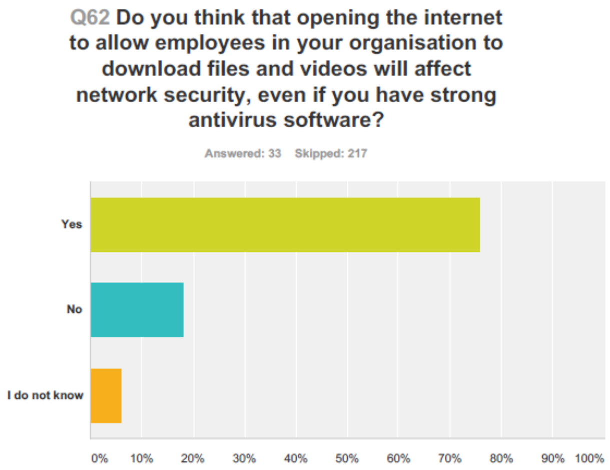
Most of the participants in the survey believe in the security system of their organisation and thinks that they have protected and secure information data centre.



70% of the participants agree that they are not allowed to use their personal routers in their respective organisations.



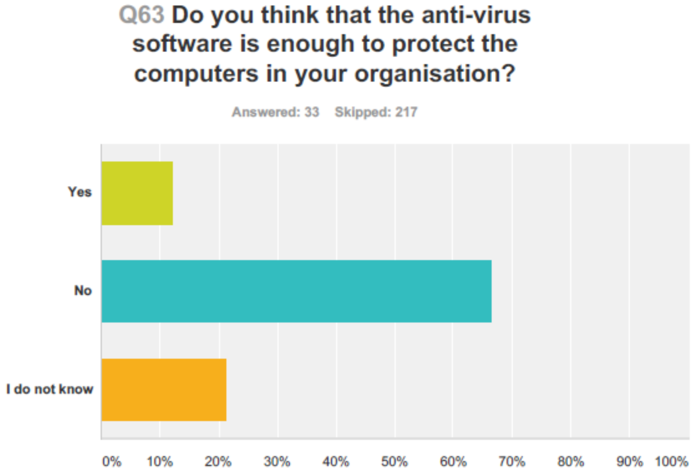
Majority of the participant have no knowledge regarding the impact of rouge access point on wireless in their respective organisation.



Q62 Do you think that opening the internet to allow employees in your organisation to download files and videos will affect network security, even if you have strong antivirus software?

Answered: 33 Skipped: 217

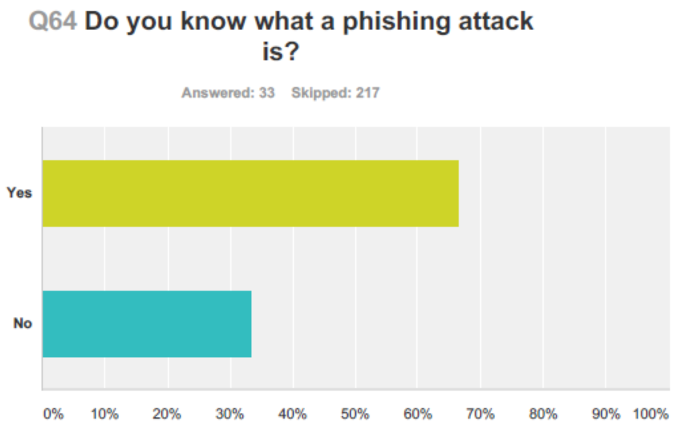
More than 80% of the participants accepts that if their organisation allow them to access wireless internet for downloading videos and files, it will affect the network security of the organisation even if the organisation have strong antivirus software.



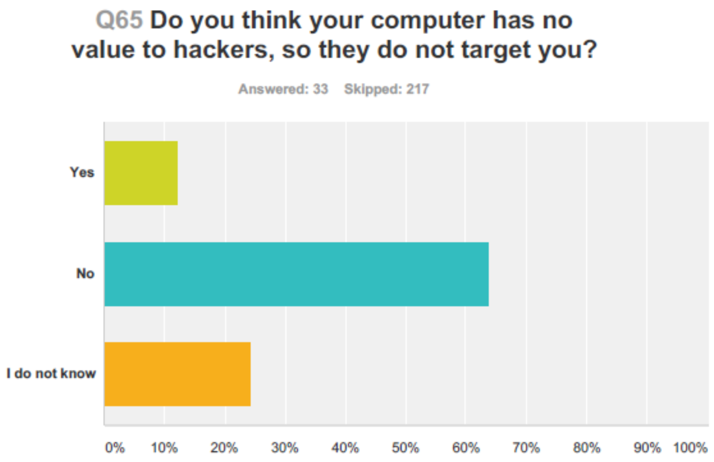
Q63 Do you think that the anti-virus software is enough to protect the computers in your organisation?

Answered: 33 Skipped: 217

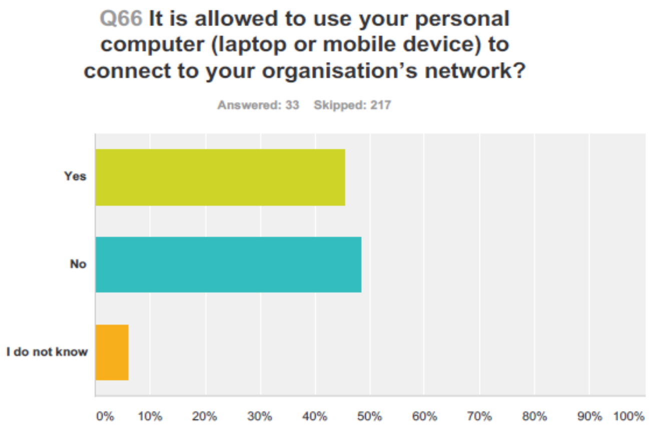
45% of the respondent believes that anti-virus software is not enough to protect the information data of the organisation.



Most the respondent working in different organisation does not know what phishing attack is and how it affects the internal information of the organisation.



50% of the respondent are unaware of the fact the hackers directly attack the main server of the organisation rather than attacking any individual’s system or personal computer.



About 50% of the respondent participated in the survey are not allowed to connect their personal pc, mobile and other electronic gadgets to organisation's network. However, about 40% of them are allowed to connect their gadgets with organisation's network.

4.2 Critical Appraisal and Further Working

It is recommended for the research to analyse the main theme of the paper in regards of its strength, weaknesses, and opportunities for further research. It is demonstrated that the main theme of the study is its main strength and it is important for the researcher to evaluate different routes in regards of maintaining its sustainability and worth. Besides, the research studies the role of information security in Saudi Arabia and it is important for the research to evaluate more literature work of different authors and scholars to form critical understanding by reviewing the main theme of the paper. It will be beneficial for the study, it the researcher make it route to evaluate different models descriptively in regards of healthcare information security framework in healthcare organisations in regards of Saudi Arabia. Moreover, it is also important for the researcher to evaluate the latest techniques and technical systems that the international healthcare information security framework uses in order to secure the data.

Furthermore, it is observed that the working of any information security system depends on its updates therefore, it is important for the researcher to continue the research regarding the working updates of the information security framework in order to maintain the work of the research study and keep it up to date respectively. On the contrary, it will be beneficial for the research study if the researcher continue to research and look for the international updates from time to time. The research strategy will increase the value of the research accordingly.

Healthcare institutions must move from a compliance posture of reviewing controls to performing upon threat intelligence as they mature their institutional incident management skills. There are different risks with the lower approaches, though just how much can be hard to explain. But those relating in threat detection, for instance, can remediate vulnerabilities more quickly than those waiting on alerts and other threat intelligence, which should review and transform their related controls or, if applying a framework, influence control updates when they happen (Stahl, 54-59).

With the support of SWOT analysis, it is appropriate to use strategic thinking regarding the IT implementation in healthcare. By observing the internal and external aspects communicating both for and against IT in healthcare, healthcare presenters can establish a strategic IT plan for establishing their data resources over the next few years. By reviewing and uncovering the concerns, policy makers can endorse modifications to establish the procedure of IT implementation simple as simultaneously working to transform the culture to improve IT advanatges for organisations and the patients and other stakeholders they serve.

Strength

Patient safety is an underlying standard of professional healthcare in the world. Establishing patient safety is an important objective at all positions of the healthcare business. The strategic initiative to enhance the IT role in healthcare can establish the cause of wider patient safety through increasing the quality of that care (Taitsman, Grimm, & Agrawal, 205-216). This study supports that IT has a vast possibility to enhance the healthcare quality and that this factor has not been completely revealed through present IT solutions.

Weaknesses

According to this research, since a patient’s cure relates obtaining services from multiple budgetary units in a healthcare institution, data system integration must exist between the computer-supported applications within a single hospital. When healthcare institutions coordinate and incorporate their internal information, they can enhance operations and decision making; though, most healthcare institutions are not yet at this position of system integration (Zhang, & Liu, 234-241). Administrative, clinical, and financial systems are not related, and as a consequence, different healthcare organisations are not yet growing their IT potential.

Opportunities

This research explained that healthcare providers and facilities are in different phases of incorporating the Internet into their activities to support new approaches to communicate with the common public, particular patients, patient groups, physicians, other providers, and staffs. Important Web-based services comprise public Web sites, different telemedicine applications for focused patient audiences, physician portals, physician education sites, and facility intranets which perform an organization’s internal audiences (Huser, & Cimino, 249-251). In general, there is an enhanced concentration throughout the healthcare sector to enhance all Web-supported applications.

Threats

This study mentioned that healthcare should use all obtainable sources to enhance patient safety and keep patient trust (Stahl, 41-44). Healthcare is a data intensive sector and the delivery of high quality healthcare depends in part on correct information, accessible at the decision point.

Areas for Future Research

IT applications in healthcare are reaching the development phase of the lifecycle. The strengths, weaknesses, opportunities, and threats at this phase of the life cycle are apparent, but some solutions have been suggested. Study is required to forecast the SWOT concerns as IT in healthcare moves from development to maturity. Case studies in both small and large physician exercises within small and large healthcare approaches are required to better consider the IT implementation costs and time-frame. Studies that focus approaches to control human obstacles to implementation are also required.

Applying the supply chain approach, the healthcare information system must be observed as to access and applicability for other presenters comprising dietitians, pharmacists, insurance companies, home health service and equipment providers, and other healthcare vendors. Patient medical information protection, information access, data security, and privacy assurances must also be observed. International suppliers and other options for outsourcing must be observed as a cost control plan.

4.3 Discussion

It is discussed in the above literature and results that IT specialist that work for the healthcare sector in different countries especially Saudi Arabia have great responsibilities to manage the data and information of their patients' confidentiality. Moreover, the discussion evaluates that the increasing complexity and complications of the information technology department make it important for different sectors to implement effective and efficient IT specialist to handle the data information related issues in an organisation. As indicated in the above discussion, it is predicted that the main issue regarding the IT department in healthcare organisation is the lack of proper implementation of IT resources that includes, the maintenance of the patient records of the hospital, the integration of different department in healthcare organisation by means of equipment like computers, portal, servers, and others, the updating procedure of the patient's data records with their previous records, the flow of data between the internal servers and department of the organisation, the lack of data backup, IT framework to manage different emergency situation, online conferencing facilities between national and international physician and their patients, and the online inventory of drugstore services in a healthcare organisation (Stahl, 141-147).

Moreover, it is observed in the above records that most of the people working in healthcare organisations and other industrial sector lacks proper knowledge regarding the role and responsibilities of IT sector in an organisation that affect their services in their respective organisation. therefore, it is important for an organisation especially health organisation to introduce different training programs for instance staff awareness programs, information data security programs and others to increase the effectiveness of their in-house employees that will further help them to increase the efficiency of their work in the healthcare sector. Besides, the complexity of the IT sector in different sectors including the healthcare sector made it important for management of the organisation to maintain the security of their information data security because all the data of healthcare organisation's patients, client, end-users, and other is save on the main server of the organisation and only a few people have permission to access them. It is also observe that these data centres have strong security system that includes continuous video monitoring to sustain the security of hospital's confidential data by external elements that further includes hackers (Taitsman, Grimm, & Agrawal, 149-161).

Furthermore, it is observed that most of the employees working in other departments of healthcare centre apart from the IT department do not even know many IT complexities that further affect the confidential data of the organisation, therefore, it is important for the organisation to provide different training programs related to IT complexities in order to maintain the working balance in the organisation along with the privacy of their patient and emergency data recovery so that healthcare organisation can maintain the sustainability of their and as well as their patient’s privacy from the hackers and other bugs that attack on the internal data of the organisation.

CHAPTER 5 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The development and use of ICT particularly networking technologies perform great responsibility to develop health care and protect patients' privacy and confidentiality. Healthcare cost is growing up considerably. A national health information system is important to enhance the efficiency, effectiveness, and quality of health care. The Kingdom spans a large geographical region and individuals move from one area to another in the country. So, a national health information system is a strategic demand and important incorporated element of any productive health care system. ICT is only one part of prerequisites to establish a national health information network for Saudi Arabia. This research concentrated on suggested system that focuses to relate all Saudi healthcare institutions to exchange medical information to give high quality standards of healthcare to the Saudi Arabia population, and, encourage movement of information despite of patient. Anticipated advantages and guidelines for implementations strategy for suggested system have been defined.

It is concluded in the above paper that IT sector plays an important role in maintain the privacy and sustainability of the organisation especially healthcare organisation. The maintenance of IT department and specialist is more important in healthcare organisation because healthcare organisation have to maintain the data of their patients and other working element with high privacy level in order to increase the reputation of their institution. Therefore, it is recommended for the hospital to maintain the level of privacy in their organisation to enhance their working capabilities in the healthcare industry.

Furthermore, the implementation of sustain and secure data centre for the healthcare sector will help the hospital to maintain the data centre of the organisation. It is observed that the most of the organisations in healthcare sector have their own data centre to secure their patients data because it work as a database for the hospital moreover, it secure all the information and medical background of their patients to use them in need. In addition, to implement IT system in healthcare organisation, it is recommended for healthcare institute to introduce different training programs for their employees in order to help them increase their working capabilities in the organisation.

The government support is observed to essential for the growth of standardisation for national health data. The normative literature missed out the assessment of various steps needed to be performed through the governments to make in blocks about the growth of national health data standards. In focusing this gap in knowledge, a qualitative, multiple-case study approach was conducted to observe the problems to the implementation of health data standards in hospitals in Saudi Arabia. Supported on the lessons observed from the hospital and the views of particular experts in the area of data exchange and standards and health informatics in Saudi Arabia, different suggestions and steps for the development of national standardisation attempts for health data was established. Last of all, healthcare organisations is one of the sector that deals with a number of end-users, privacy and security issues, patients, shareholders, and other therefore, an efficient IT specialist team is the main need of the healthcare institutions nowadays as it helps them to maintain the sustainability of data information privacy of organisation and it will benefit the institution different advantages like the flow of data in different departments of the healthcare institution. It will also help the organisation to maintain the communication gap among the end-users of the organisation and this benefit will help the organisation to enhance their working capacities in the market place.

5.2 Recommendations

The government of KSA has correctly concluded that ICT will be an increasingly essential underlying fabric influencing all elements of a society and will impact its future economic development. How the resilience and security functions of ICT and the information systems supporting important infrastructures are established, operated and observed for threats to their operations within KSA will also impact perceptions of KSA by other countries within the international community, who are also focusing same problems. This research is focused on the information security efforts important for securing ICT, information systems and information. Within today’s world, ICT and information systems give important services and functions that impact the operations of a nation’s national security systems, government institutions, and private enterprises. As operational dependency on the ICT and electronic systems enhances, information security risks become further important. Information security is not just an important supporting function but it should also give countermeasures to vulnerabilities that can be exploited. Moreover, the implementation of the ICT, information systems, applications and operational procedures impact the reliably, availability, and sustainably of those “critical” functions and services in the face of disruptive events. One of the overarching goals for the KSA is to give a strategy and support for getting a suitable and sustained level of ICT security. Every infrastructure operates within an exclusive set of requirements and collectively they participate to national security and financial security at different levels of criticality. Most important infrastructures, comprising those that perform national security tasks, though normally fewer in number, perform and encourage the most essential and basic role a government should practise; namely, confirming national sovereignty and security of its people. Government services and functions, like emergency services, are very important and different Government services are supported by its people for important services and the orderly functioning and financial health care of the KSA. Different private institutions (but not all) give some nationally important operations and services that underpin the productive operations of government institutions, other private organisations’ operations and a vast array of services to the people of KSA.

It is essential that important infrastructure protection and resilience be believed a particular element of an overall national security plan. A particular Critical Infrastructure Security and Resilience Strategy (CISRS) for KSA must be established. It should concentrate on both the physical safety of major assets and the safety of ICT and information systems applied within critical infrastructures. Without an inclusive system, there can be no guarantee that infrastructure security and resilience is being applied and operated commensurate with recognised national-level hazards and interdependencies. This research focused the resilience and security needs for ICT and information systems. Though the assessment recognised different particular independent infrastructure attempts connected to organisational and technical infrastructure, no evidence was there about an inclusive national critical infrastructure protection plan.

Work cited

Abdelhak, M., Grostick, S., & Hanken, M. A. (2015). Health information: management of a strategic resource. Elsevier Health Sciences.

Agaku, I. T., 2014. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. Journal of the American Medical Informatics Association, 21(2), pp. 374-378.

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. Journal of the American Medical Informatics Association, 21(2), 374-378.

Altuwaijri, M. M. (2008). Electronic-health in Saudi Arabia. Just around the corner? Saudi medical journal, 29(2), 171-178

Anderson, J. G. (2007). Social, ethical and legal barriers to e-health. International journal of medical informatics, 76(5), 480-483

Appari, A., 2010. Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), pp. 279-314

Bah, S., Alharthi, H., El Mahalli, A. A., Jabali, A., Al-Qahtani, M., & Al-kahtani, N. (2011). Annual survey on the level and extent of usage of electronic health records in government-related hospitals in Eastern Province, Saudi Arabia. Perspectives in health information management/AHIMA, American Health Information Management Association, 8(Fall).

Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 103-114)

Blumenthal, D. (2009). Stimulating the adoption of health information technology. New England Journal of Medicine, 360(15), 1477-1479.

Blumenthal, D., & Tavenner, M. (2010). The meaningful use regulation for electronic health records. New England Journal of Medicine, 363(6), 501-504

Cervesato, I., 2012. Trace matching in a concurrent logical framework. In Proceedings of the seventh international workshop on Logical frameworks and meta-languages, theory and practice. ACM., pp. 1-12

Chen, D., 2012. Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering. International Conference onIEEE. Volume 1, pp. 647-651

Chen, T. L., Chung, Y. F., & Lin, F. Y. (2012). A study on agent-based secure scheme for electronic medical record system. Journal of medical systems, 36(3), 1345-1357

Cholleti, S., Post, A., GAO, J., Lin, X., Bornstein, W., Cantrell, D., & Saltz, J. (2012). Leveraging derived data elements in data analytic models for understanding and predicting hospital readmissions. In AMIA Annual Symposium Proceedings (Vol. 2012, p. 103). American Medical Informatics Association

Davis, K., Doty, M. M., Shea, K., & Stremikis, K. (2009). Health information technology and physician perceptions of quality of care and satisfaction. Health Policy, 90(2), 239-246.

El Din, M. N. (2007). Physicians' use of and attitudes toward Electronic Medical Record System implemented at a teaching hospital in Saudi Arabia. The Journal of the Egyptian Public Health Association, 82(5-6), 347-364

Gordon, L. A., 2002. The economics of information security investment. ACM Transactions on Information and System Security, 5(4), pp. 438-457

Höne, K. & Eloff, J. H. P., 2002. Information security policy—what do international information security standards say? Computers & Security, 21(5), pp. 402-409

Huser, V., & Cimino, J. J. (2013). Don't take your EHR to heaven, donate it to science: legal and research policies for EHR post mortem. Journal of the American Medical Informatics Association, amiajnl-2013

Kahn, J. S., Aulakh, V., & Bosworth, A. (2009). What it takes: characteristics of the ideal personal health record. Health affairs, 28(2), 369-376

Karlsson, F., 2014. Practice-Based Discourse Analysis of Information Security Policy in Health Care. In The 11th Scandinavian Workshop on E-government -Linköping University..

Khalifa, M. (2013). Barriers to health information systems and electronic medical records implementation. A field study of Saudi Arabian hospitals. Procedia Computer Science, 21, 335-342.

Maxwell, J. A. (2012). Qualitative research design: An interactive approach: An interactive approach (Vol. 41). Sage.

McKibbon, K. A., Lokker, C., Handler, S. M., Dolovich, L. R., Holbrook, A. M., O'Reilly, D., & Roshanov, P. S. (2012). The effectiveness of integrated health information technologies across the phases of medication management: a systematic review of randomised controlled trials. Journal of the American Medical Informatics Association, 19(1), 22-30.

Merriam, S. B. (2014). Qualitative research: A guide to design and implementation. John Wiley & Sons.

Moore, A. P., 2001. Attack modeling for information security and survivability. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INS.

Murdoch, T. B., & Detsky, A. S. (2013). The inevitable application of big data to health care. Jama, 309(13), 1351-1352.

Silverman, D. (2013). Doing qualitative research: A practical handbook. SAGE Publications Limited.

Smith, E., 1999. Security in health-care information systems—current trends. International Journal of Medical Informatics, 54(1), pp. 39-54.

Stahl, B. C., 2012. Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal, 22(1), pp. 77-94.

Stefanidis, D., 2012. Simulator training to automaticity leads to improved skill transfer compared with traditional proficiency-based training: a randomised controlled trial. Annals of surgery, 255(1), pp. 30-37.

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. New England Journal of Medicine, 368(11), 977-979.

Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. The Journal of Strategic Information Systems, 16(2), 130-152.

Wager, K. A., Lee, F. W., & Glaser, J. P. (2009). Health care information systems: a practical approach for health care management. John Wiley & Sons.

Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user’s perspective. Health informatics journal, 18(3), 191-201

World Health Organisation. (2010). World health statistics 2010. World Health Organisation.

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference (pp. 268-275)

APPENDIX

Questionnaire

This study is being undertaken as part Master Degree study for ….. The research is sponsored by the Ministry of Health in Saudi Arabia. The purpose of this research is to develop a framework to protect the data and information in the healthcare sector in Saudi Arabia. As a researcher, I would like to put this questionnaire in front of you to participate in this study. This study will benefit for the data and information security in healthcare sector in Saudi Arabia as it will provide solutions to overcome barriers in order to save the data sensitive of patients and employees.

Personal Data for all participants

Gender

A- Male

B- Female

Which of the following department do you work in?

- Department of Medicine
- Department of Surgery
- Administration
- Acute assessment unit
- Burn centre
- Central sterile services department
- Coronary care unit
- Emergency department
- Geriatric intensive-care unit

- Hospital pharmacy
- Hospital warehouse
- Intensive care unit
- Medical records department
- Neonatal intensive care unit
- On-call room
- Operating room
- Pediatrics intensive care unit
- Physical therapy
- Post-anaesthesia care unit
- Psychiatric hospital
- Release of information department

Length of Service

A- 1-2 years

B- 2-5 year

C- More than 5 years

For IT team

Awareness Training staff:

Do you have any relevant staff training program in your organisation?

A- Yes
B- No
C- Don't Know

Do you have any system of maintaining user awareness of information and data security risks?

Do you have clear account management processes emplace in your hospital, with a strong password protection and a limited number of privileged accounts?

Monitoring:

1- Do you think your organisation monitor user activity, and control access to activity and audit logs?

   A- Yes

   B- No

   C- I do not know

King Fahad Medical City

2- Do you think your organisation continuously monitors activity on ICT systems and networks, including for rogue wireless access points?

   A- Yes

   B- No

   C- I do not know

3- Do you analyse network logs in real time, looking for evidence of mounting attacks?

   A- Yes

   B- No

   C- I do not know

Polices:

4- Do you think your organisation have a policy controlling mobile and removable computer media?

   A- Yes

   B- No

   C- I do not know

5- Do you think your organisation have an incident response and disaster recovery plan and policies?

   A- Yes

B- No

C- I do not know

6- Do you have an appropriate anti-malware system and practices that are effective against likely threats?

A- Yes

B- No

C- I do not know

Testing:

7- Do you know penetration testing?

A- Yes

B- No

8- Do you protect its networks against internal and external attacks with firewalls and penetration testing?

A- Yes

B- No

C- I do not know

9- Do you think your organisation monitor and test security controls?

A- Yes

B- No

C- I do not know

10- Do you know what a Social Engineer is?

A- Yes

B- No

Scan:

Do you continuously scan for new technical vulnerabilities?

A- Yes

B- No

Do you scan for malware before allowing connections to your systems?

A- Yes

B- No

Do you continuously scan the network and attachments for malware?

A- Yes

B- No

Is it tested for readily identifiable compromise scenarios?

A- Yes

B- No

11- Does your organisation have Integrated Delivery System IDS/IPS systems?

A- Yes

B- No

C- I do not know

Physical

12- The Data Centre (DC) in your organisation is available for anyone to access?

A- Yes

B- No

C- I do not know

13- The Data Centre (DC) in your organisation is available for anyone from IT team to access?

A- Yes

B- No

C- I do not know

14- Is the Data Centre has camera monitoring?

A- Yes

B- No

C- I do not know

15- Are there any records of which anyone access the Data Centre (DC)?

A- Yes

B- No

C- I do not know

16- Does your organisation have physical backup of Data Centre (disaster recovery)?

A- Yes

B- No

C- I do not know

17- Do you think that you are familiar with servers and security devices that under your responsibility?

A- Yes, with all of them.

B- Yes, with most of them

C- No

18- Does your organisation implement Demilitarized Zone DMZ?

A- Yes

B- No

C- I do not know.

19- Do you think your organisation is protected and more secure?

A- Yes

B- No

C- I do not know

20- Is it allowed in your organisation to use personal router (wireless internet device)?

A- Yes

B- No

C- I do not know

21- Do you think the rouge access point will impact on wireless in your organisation?

A- Yes

B- No

C- I do not know

22- Do you think that the anti-virus is enough to protect the computers in your organisation?

A- Yes

B- No

C- I do not know

23- Do you think that when you open the internet to allow employees in your organisation to download files and videos will affect the network security even if you have strong antivirus?

A- Yes

B- No

C- I do not know

24- Do you know what a phishing attack is?

A- Yes,

B- No,

25- Do you think your computer has no value to hackers, so they do not target you?

A- Yes

B- No

C- I do not know

26- It is allow using your personal computer (lab top or mobile device) to connect in your organisation network?

A- Yes,

B- No,

C- I do not Know

27- Have you downloaded and installed software on your computer at your work?

A- Yes,

B- No,

C- I do not know

28- Do you think you are familiar with all IT devices under your section (computer, Scanner, Fax & printer)?

A- Yes,

B- No

C- I do not know

End user:

1- Which one of these examples is stronger password?

A- Ahmed1982

B- Father12@

C- Secure159

D- Ler!45sfe

2- Which of the following is a correct of an email address?

A- www.yahoo.com

B- Ahmed@yahoo.com

C- Divid.gmail.com

D- www.hotmail.com

3- What is the best way to keep your password more secure from disclosure?

A- I will memorise it.

B- I will write it down only.

C- …

D- …..

4- What should you do if someone from IT team asks you for your password?

A- Since he is from IT team, I will give him.

B- I will contact with my leader.

C- I will never give to anyone even IT Team.

D- If I have issue in my PC then I give to him.

5- Which are of the following offer email service?

A- Yahoo and Google.

B- Amazon and Google.

C- Twitter and Facebook.

D- Hotmail and Facebook.

6- Information Security in healthcare is an important, who do you think is responsible for information security in your organisation?

A- IT Services

B- Departments that use data

C- Managers and team leaders

D- Individual employees

7- If someone e-mails you an attachment/link that is not work related, how likely are you to open it?

A- Not likely

B- Possibly, depending on what is being sent

C- Very likely

D- Always

8- Has anyone you know at work asked for your password?

A- Yes and I provided it

B- Yes and refused to provide it

C- No

9- Have you saved files in your organisation’s desktop?

A- Always

B- Sometimes

C- Rarely

D- Never

10- Do you know the shard folder and its advantage?

A- I have not used it.

B- I always use shard folder.

C- I know it but not use it.

D- I do not know the shard folder.

Training Awareness

11- I have received Information Security awareness training in your organisation?

A- Yes

B- No

12- I have received Data Protection awareness training at the University?

A- Yes

B- No

13- I have signed a pledge not to disclose the private information and data of the organisation?

A- Yes

B- No

14- What is the state of security awareness training in your organisation?

A- Strong.

B- Good.

C- Weak

D- No training.

15- Do you think the information security relevant to IT team only?

A- Yes

B- No

C- I do not know.

16- Do you think that you need basic security awareness training when you join your organisation?

A- No, because I have basic information security.

B- No, because it is not under my responsibility.

C- Yes.

D- I do not know.

17- When leaving for lunch or to take a break, how do you secure your computer?

A- I turn my monitor off

B- I log off

C- I lock the computer

D- I turn the computer off

E- None of the above

Knowledge of Information Security:

18- Do you think sharing games or programs with your co-workers will impact on the information security in your organisation?

A- Definitely no impact.

B- It will impact.

C- I do not know.

19- There are many websites offering to help in private chat? Do you think there are secure to deal with them?

A- Yes

B- No

C- I do not know

20- How do you know that your origination's computer is secure?

A- Contact information security team.

B- Check the Anti-virus setting.

C- Check with my leader.

D- It's not my business.

21- How do you know that the Anti- virus software is enabling?

A- Check the Anti-virus setting

B- Check with my leader.

C- It should be enabled.

D- Contact information security team.

22- What can you do if you fall victim to data theft?

A- Check the Anti-virus.

B- Check with my leader.

C- Contact information security team.

D- Information security team will know about that.

23- Do you think that the protection of data is one of your roles and responsibilities in your work?

A- Yes

B- No

C- I do not know

24- Are you agreeing to the basic information about how to protect the data in your organisation?

A- Yes, Strongly.

B- Yes, if there like

C- It is not my responsible.

D- I do not know.

25- Do you think healthcare information system (HIS) is important in organisation healthcare?

A- Very important

B- Important

C- Not important

D- Healthcare can work without HIS.

26- The Social Engineer is a person that will talk people into revealing passwords or information that will compromise the company security. If you face this case, what you will do?

A- I will ignore him.

B- I will advise him to leave this way.

C- I will tell IT team.

D- I will tell my leader.

27- Do you think that the IT team in your organisation is high qualified to make your organisation more secure?

A- Yes

B- No

C- I do not know

28- Do you think that the anti-virus is enough to protect the computers in the organisation?

D- Yes

E- No

F- I do not know

29- Do you know what a phishing attack is?

C- Yes, I do

D- No, I do not

30- Do you think your computer has no value to hackers, so they do not target me?

D- Yes, they do not target me

E- No, they will target me.

31- It is allowed using your personal computer (lab top or mobile device) to connect in your organisation network?

D- Yes, it is allow

E- No, it is not allow

32- Have you downloaded and installed software on your computer at your work?

D- Yes, I have

E- No, I have not.

33- Do you use the same passwords for your work accounts as your do at home, Facebook and Twitter?

A- Yes, I do

B- No, I do not.

34- When you delete a file from your computer, that file can no longer be recovered?

A- Yes

B- No