

**SECURE MANAGEMENT OF ICT RESOURCES FOR A
UNIVERSITY: THE CASE OF KAMPALA
INTERNATIONAL UNIVERSITY**

BY

KORIR AMOS KIPKOSGEI

MCI/3809/72/DF

**A Dissertation Submitted to the School of Postgraduate Studies as a
Partial Fulfillment of the Requirements for the Award of Degree
of the Masters of Science in Information Systems of
Kampala International University**

MARCH 2010

DECLARATION

I Korir Amos Kipkosgei do declare that this research is my original work and has not been published or submitted for any other academic award of any other university before


Signed:
Korir Amos Kipkosgei

Date: 26/05/2010.

APPROVAL

This research was conducted and a report written with my approval as the student's supervisor.

Signed: 

Date: 

Mr. Bada Joseph Kizito

(Supervisor)

DEDICATION

I dedicate this work to my parents Mr. and Mrs. Twei, my siblings, my friends and all my colleagues.

ACKNOWLEDMENT

I would like to thank the Almighty God for every opportunities He has provide and especially being able to study and also for future opportunities.

Special acknowledgement to my parents and relatives for their spiritual, moral and financial support they provided all through my studies. I also acknowledge my siblings for believing in me.

I acknowledge my supervisor Mr. Bada Joseph and the academic staff of School of Computer Studies of KIU for their support and guidance through the research. They played a role and provided me with the encouragement towards the success of this work.

I would like to acknowledge the staff of the department of ICT of KIU for their support given and contributing in the research

Finally, to my colleagues Maganda Evans and Businge Phelix for the friendly and advice they provide all through our study.

TABLE OF CONTENTS

COVER PAGE.....	i
DECLARATION	ii
APPROVAL	iii
DEDICATION.....	iv
ACKNOWLEDMENT	v
TABLE OF CONTENTS.....	vi
LIST OF FIGURES	x
ABSTRACT.....	xi
CHAPTER ONE: INTRODUCTION.....	1
1.1 Background of the Study	1
1.2: Statement of the Problem.....	2
1.3: Objectives of the Study.....	3
1.3.1: General Objective	3
1.3.2: Specific Objectives	3
1.4: Research Questions.....	3
1.5: Scope of the Study	4
1.6: Significance of the Study.....	4
1.7: Conceptual framework.....	5
CHAPTER TWO: LITERATURE REVIEW	9
2.1: Information Communication Technology	9
2.2: Computer security.....	10

2.2.1: Information Security, ICT security and ICT security management.....	10
2.2.2: Information Security Characteristics and Models	12
2.3: Internet related ICT insecurity	15
2.4: Security Domains.....	16
2.5: ICT security in institution of higher learning case of Georgetown University	17
2.6: Challenges of ICT Security in Higher Education	18
2.7: ICT security in developing countries the case of Tanzania	20
2.8: ICT security management in non-commercial organizations	22
2.9: Conclusion	23
CHAPTER THREE: METHODOLOGY	25
3.0: Introduction.....	25
3.1: Study Area	25
3.2: Description of the study population.....	25
3.3: Research design	25
3.4: Methods of Data Collection.....	26
3.4.1: Interviews.....	26
3.4.2: Observation.....	26
3.4.3: Questionnaires	27
3.5: Data analysis method.....	27
CHAPTER FOUR: FINDINGS AND ANALYSIS	28
4.0: Overview.....	28
4.1: Data analysis	28
4.2: Population of the study	28

4.3: Results and Analysis of Findings.....	29
4.3.1: ICT facilities available.....	29
4.3.2: Management of ICT Facilities (Security Management)	30
4.3.3: Use of password as the access control mechanism.....	32
4.3.4: Protection against viruses	33
4.3.5: Maintenance of ICT facilities	38
4.3.6: Data backup	40
4.3.7: ICT security measures	42
4.4: Improvement of ICT security	43
4.4: Current ICT security issues.....	44
4.4.1: Viruses, worms and Trojans.	44
4.4.2: System crash	45
4.4.3: Data back up	45
4.4.4: Use of pirated software	45
4.5: SWOT analysis of management of ICT security in KIU	46
CHAPTER FIVE: DISCUSSION, RECOMMENDATIONS AND CONCLUSION.....	48
5.0: Overview.....	48
5.1: Discussion.....	48
5.2: Recommendations.....	50
5.2.1: Proposed framework for ICT security for Kampala International University	50
5.3: Conclusion	56
5.4: Future research.....	57
5.5: Limitations of the research	57

REFERENCES 58

APPENDICES 61

APPENDIX A: Questionnaire: 61

APPENDIX B: Interview guide:..... 65

Appendix C: Observation Checklist 66

LIST OF FIGURES

Figure 1: Conceptual framework for ICT security in KIU	7
Figure 2: Response on whether someone in charge of ICT security within departments	21
Figure 3: Analysis on whether someone in charge of ICT security management	22
Figure 4: Response of use of password as an access control mechanism	23
Figure 5: Analysis of passwords as access control mechanism	24
Figure 6: Departmental response on antivirus update.....	25
Figure 7: General response on installation of antivirus on computers	25
Figure 8: Frequency of antivirus update in different departments	26
Figure 9: general response on antivirus of antivirus	27
Figure 10: Frequency of virus scan according to respondents	28
Figure 11: Analysis of the general response on virus scan	29
Figure 12: Response on frequency of ICT facilities maintenance	29
Figure 13: analysis of response on maintenance of ICT facilities	31
Figure 14: Response on availability of back up mechanism within to departments	32
Figure 15: Analysis of availability of data backup mechanism	32
Figure 16: An analysis of data backup frequency.....	33
Figure 17: Respondents on knowledge of existence ICT security measures.....	34
Table 1: SWOT analysis table for KIU ICT security	36

ABSTRACT

Information and Communication Technology (ICT) is one of the keys pillars in development in the current society. Every institution or company uses ICT facilities and services to carry out their day to day activities. For this reason the security of these services and facilities is very important. An institution which has a proper and reliable ICT security management stands good chances of continuity and on the other hand poor ICT security spells out doom to the company.

Institutions of higher learning like Kampala international University (KIU) ICT is of strategic importance especially in management and online learning. The security of information being processed stored and exchanged needs to be clearly elaborate as the dependence on ICT on most institutions core services is increasing.

This research report is organized into five chapters and it highlights the current state of ICT security in institutions focusing on KIU. It includes the challenges being encountered and a framework which if implemented then a positive change can be achieved in managing ICT security

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Kampala International University (KIU) is one of the private and fastest growing universities in Uganda which began its operations in 2001. It has grown both in terms of population and facilities. KIU has two campuses currently within Uganda; the main campus in Kampala along Kansanga Ggaba road and the Western campus in Ishaka Bushenyi district which mainly offer medical related courses. It attracts students from the East African region and beyond. Its vision is to become a premier institution of international repute that prepares students for the world and for an inclusive society

In terms of Information and Communication Technology (ICT), KIU has well advanced in it. There are various ICT facilities within the institution including computers, printers, photocopiers, computer networks, internet services among others. The main purpose of these facilities is data processing and information storage. Majority of the institution's departments at least has an ICT facility. The institution has an ICT department which is in charge of everything concerning ICT in the university. There are also several computer labs well equipped with computer systems used for both learning and research purposes.

Due to the importance of these ICT facilities and services, there security should be ensured to guard against data loss, theft, vandalism, catastrophes or anything that poses an ICT security threat. The data processed and stored by these ICT facilities is very important. Information provides the basis of any institution and also ensures continuity of

any business, thus it needs to be secure, and at the same time available when needed and most of all reliable.

1.2: Statement of the Problem

Cases of ICT insecurity have increased and become common of recent. ICT facilities have been use both as subject of attacks and object of attacks by unauthorized individuals. Various Universities have experienced such cases like hacking into results and transcripts processing systems and other vital areas.

KIU also being an institution of higher learning, and ICT being one of the essential components for successful business, its ICT security needs to be clearly defined and ensured. There should be clear measures and guidelines concerning ICT security in place which are well understood and available to the whole KIU community. More than that, they should be enacted.

It is therefore on this basis that the researcher is came up with this research, to analyze the state of ICT security and establish the minimum requirements to ensure ICT security in KIU is well addressed.

1.3: Objectives of the Study

1.3.1: General Objective

Though ICT had been very well embraced in KIU and its security fairly maintained, there was never a report that gives a full account of the ICT security impact on information and the users. The main objective of the research was to carry out a comprehensive analysis of ICT security in KIU, which was establish the extent to which information was secure and at the same time available. The study defined ICT security requirements desirable, and a framework for meeting them

1.3.2: Specific Objectives

To achieve the aim of the study, the specific objectives were to:

- i. Investigate on the current status of security on ICT systems of KIU.
- ii. Analyze its impact on information systems, based on their confidentiality, Integrity and Availability.
- iii. Establish the desirable ICT security requirements for ICT systems in KIU
- iv. Establish a framework for meeting these ICT security requirements to be adopted by the institution.

1.4: Research Questions

The questions which guided the researcher were;

- i. Are there any ICT security measures in place?

- ii. How is security of information systems ensured in terms of its Confidentiality, Integrity and Availability?
- iii. How can the security of ICT systems in KIU be improved?

1.5: Scope of the Study

The study was carried out in Kampala International University main campus at Kansanga, Kampala. It will cover the entire ICT security system i.e. all the areas where computer and information security is vital. However, more emphasis was on the school of computer studies and the department of ICT.

School of computer studies was on the focus because, KIU being an institution of higher learning, it is this school which is mandated to impart knowledge concerning IT issues, and so it is deemed to be of help in the study. Department of ICT on the other hand is the body given the responsibility of managing ICT systems within the university, i.e. formulating appropriate policies and implementing them for the smooth and efficient running of these systems. Also any recommendations which will come out of the study will be of much importance to the ICT department.

The study was carried out and completed within five months of which it was ready for presentation.

1.6: Significance of the Study

The study has the following importance;

- i. Confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.
- ii. The hardware and software components that constitute the university's IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.
- iii. The use of university IT assets in other than in a manner and for the purpose for which they were intended represents a misallocation of valuable university resources, and possibly a danger to its reputation or a violation of the law.
- iv. Proper functionality of IT systems is required for the efficient operation of the university.
- v. Finally the study is important to the researcher as it one of the requirements for the award of a masters degree in information systems

1.7: Conceptual framework

ICT security is not a very new idea in institutions of higher learning. Since they use a lot of ICT facilities and services, the issue of security is often faced. First a lot of incidences of security breach is experienced of which some may be minor while others are might major and be catastrophic. These breaches range from mere sharing of passwords, breaking to systems and even hacking into systems which critical information

Also there is the idea of securing ICT systems from these threats or security breaches. Every institution tries to come up with measures to ensure that their systems are secure enough and that common security threats are cubed. These measures at times include implementing the use of access controls like passwords to prevent unauthorized access to systems. Installation of antivirus software on computer systems in order to secure information is another way. In some instances, also restricting access to certain rooms is used as a measure.

In cases or instances where security measures are not in place, then there is a danger. Threats to ICT security are real and can cause untold destruction of which some of the effects could be irreversible. Some of these effects could be data loss, data ending up in wrong hands or theft of ICT facilities

On the other hand, when ICT security is well ensured, then there is a lot to benefit from. A secure ICT system will ensure confidentiality, integrity and availability of information. It will also ensure safety of the ICT facilities. To the institution as a whole a good ICT security management will keep it at a competitive edge in the market, growth and gaining trust from the public.

ICT security is important to both the ICT facilities and also the users of these facilities. Actually at the end of the day it is the personnel who benefit more. It is possible to achieve efficient security management but you cannot achieve perfect security. This is so

because as much security is needed also availability of these ICT facilities and services to the authorized individuals and systems is equally important.

For the case of KIU the diagram below can illustration the need for security

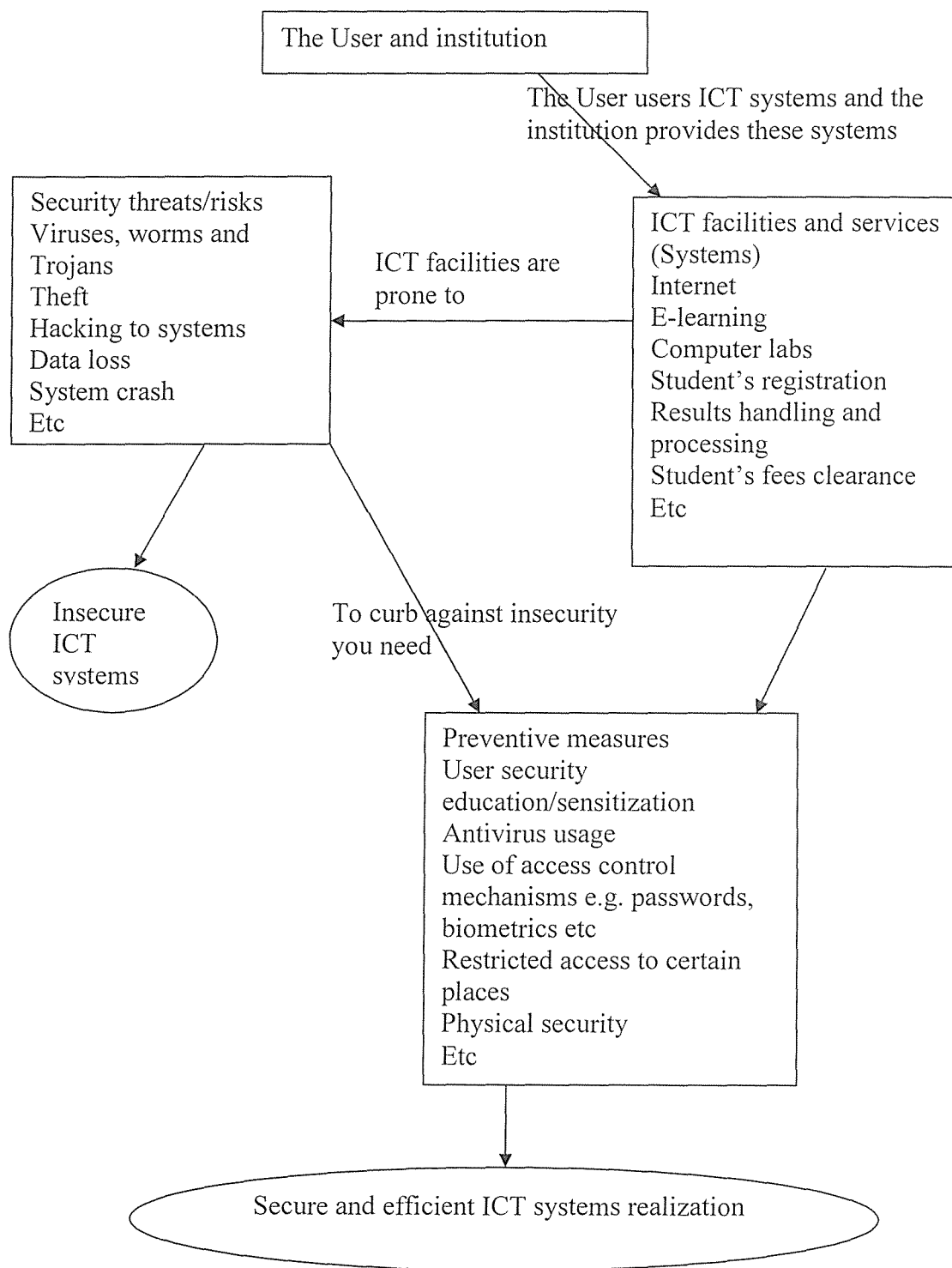


Figure 1: Conceptual framework for ICT security in KIU

CHAPTER TWO: LITERATURE REVIEW

2.1: Information Communication Technology

Information and communication technology (ICT) is the basis for our modern society. Without PCs, supercomputers, fibre optic cables, wireless networks, microchips and the many other forms of ICT, both society and research would be very different to the reality in which we live today.

ICT are central to modern life. They are increasingly used at work, in day-to-day relationships, to access everything from public services to culture and entertainment, and for community and political participation. Unfortunately not everybody fully benefits. For instance, anything from 30-50% of all Europeans still gain few or none of the ICT-related benefits. The main reasons are lack of access to equipment or networks, the limited accessibility of user-friendly technologies, price, motivation, limited skills and different generational attitudes to advanced technologies.

ICT has become a foundation of modern society. Many countries now regard the understanding of ICTs and the mastering of basic skills and concepts within ICTs as part of the core of education in their country, alongside reading and writing (UNESCO, 2002). ICT is an umbrella term encompassing any communication device or application and the various services and applications associated with them. European Commission claims that the importance of ICT lies more in its ability to create greater access to information and communication in underserved populations than in the technology itself.

2.2: Computer security

Security can be defined as the quality or state of being secure or free from danger. Albion.com website defines computer security as the ongoing and redundant implementation of protections for the confidentiality and integrity of information and system resources so that an unauthorized user has to spend an unacceptable amount of time or money or absorb too much risk in order to defeat it, with the ultimate goal that the system can be trusted with sensitive information. The scope of computer security has grown from just physical security to include safety of data, limiting unauthorized access to the data and involvement of personnel from multiple levels of the organization. A successful organization should have multiple layers of security in place. These layers include physical security, personal security, operations security, communication security and network security.

It is practically impossible to achieve perfect security because security is not absolute but a process. Security should be balanced between protection and availability. To achieve the balance, the level of security must allow access yet protect from threats.

2.2.1: Information Security, ICT security and ICT security management

Information security implies safe guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. On the other hand ICT security is concerned about Confidentiality, Integrity and Availability of information whether in storage, processing or transit (Bakari, 2007). Information security and ICT security and sometimes used interchangeably. Bakari (2007) in his paper defines

ICT security management as the overall process of establish an adequate ICT security within an organization in order to achieve the appropriate levels of Confidentiality, Integrity and Availability (CIA)

Keeping vital information secure is imperative to all organizations. This is done by practicing information security, and the work must start with a management supporting the co-workers and also by educating end users and organization members in information security. Information security is about protecting information from accidents, breaches or other events that could make it harder to understand the information. Information security is practiced in organizations that tend to rely on information, and a certain lack of information could harm the organization. Virtually this is imperative in all organization in this day and age. This means that information security is important to any institution.

Institutions of all sizes collect and store huge volumes of confidential information. The information may be about employees, customers, research, products or financial operations. Most of this information is collected, processed and stored on computers and transmitted across networks to other computers. If this information fell into the wrong hands, it could lead to lost business, law suits, identity theft or even bankruptcy of the business.

Information security has evolved significantly and grown even more important in recent years. From a career perspective, there are even more areas where a professional can work in the field. Some of the specialty areas within Information Security include

network security, application and database security, security testing, information systems auditing, business continuity planning and digital forensics science, among others.

The notion of information security has been standardized and defined by ISO, more specifically by the standard ISO/IEC 17799. This standard provides guidelines that information security management can find useful. The ISO/IEC standard 17799 (International Standard for IT security known as Information Technology – Code of Practice for Information Security Management) defines information security within three terms; Secrecy (Confidentiality), Integrity and Accessibility/Availability. Secrecy/Confidentiality deals with the notion that information should only be available to those with right authority to read and use the information. Steps are needed to ensure that no unauthorized use occurs. The integrity of information regards protecting the information so that it is accurate, complete and correct. Lastly, the accessibility/availability of information concerns ensuring that users have access to the information they need when they need it without delays.

2.2.2: Information Security Characteristics and Models

Information security has become a commonly used concept, and is a broader term than data security and IT security (Björck, 2001). In the society of Information Age, security of information plays a central role in several domains with different scopes and objectives such as: Privacy of personal data in an institution; Integrity of transaction and business continuity in the business domain; and defending democracy in the e-government domain. In earlier research, it has been shown that measures to achieve information security in the administrative or organizational level are missing or

inadequate. Therefore, the need to improve information security models by including vital elements of information security is turning to be more serious. In the last decades, due to the spread of ICTs, governmental organizations and communities of academics and practitioners have developed security models for evaluating products, and setting up security specifications in order to prevent incidents and reducing the risk of harm.

According to the context of IS/IT, information security is a concept that is becoming widely used. Information is dependent on data as a carrier and on IT as a tool to manage the information; hence, information security has an organizational focus. The U.S. National Information Systems Security Glossary (2006, p 33) defines information system security as: “The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats”.
Characteristics of Information Security In order to improve the understanding of the concept of information security, the characteristics of information security must be seen as a success. The relation emphasizes that both concepts need to be taken into account, and that it is necessary to address all four characteristics of information security before claiming that information security has been achieved.

Information security concerns security issues in all kinds of information processing and includes the following four characteristics: Availability, Confidentiality, Integrity and Accountability. According to SIS (2003) information security is defined as the protection

of information assets, aiming to maintain confidentiality, integrity, availability and accountability of information. Availability concerns the expected use of resources within the desired time frame. Confidentiality relates to data not being accessible or revealed to unauthorized people. Integrity concerns protection against undesired changes. Accountability refers to the ability of distinctly deriving performed operations from an individual. The Model Both technical and administrative security measures are required to achieve these four characteristics. Administrative security concerns the management of information security; strategies, policies, risk assessments etc. This part of the overall security is thus at an organizational level and concerns the institution as a whole. It is positioned towards what the overall security requirements should be. Technical security concerns measures to be taken in order to achieve the overall requirements. Technical security is subdivided into physical security and IT security. Physical security concerns the physical protection of information, for instance, fire protection and alarm. IT security refers to security for information in technical information systems. IT security can then be subdivided into computer- and communication security. Computer Security concerns the protection of hardware and its contents while Communication Security involves the protection of networks and other media that communicate information between computers. In order to provide a more understandable view of how these characteristics and security measures relate to one another, an information security model has been created.

2.3: Internet related ICT insecurity

With internet age, information revolution has been experienced a lot. ICT and generally digital insecurity emerged and we can identify the following key security issues related to the information revolution:

Intangibility of Information

Digital information exists independently from the physical tools that carry information. And information cannot be absolutely contained — it is easily disseminated, copied, modified, destroyed, or stolen. The negative effects of this flexibility include information theft, identity theft, and intellectual property theft.

Complexity of ICT Systems

Every ICT system contains bugs (i.e. software or hardware faults) and the more complex an ICT system is, the more bugs it contains. Not all bugs compromise security, but those that do can be exploited by potential attackers. An ICT system's security is difficult to control and manage. ICT systems interact with other systems and with people, and some of their features (and vulnerabilities) were never anticipated when they were originally designed.

Automation

One important property of computers is the huge potential for automation. Computer programs can automate many arduous tasks and thus provide a high degree of efficiency

and accuracy. But automation can also ease and speed up the process of breaking into an ICT system.

Global Networking

In the real, physical world attacks occur at specific geographical locations. In the world of global networks, however, attackers can connect to the Internet from any computer anywhere in the world and reach any other online system, regardless of its physical location. This global connectivity makes attacking easier and less resource-intensive; also, maintaining anonymity is relatively easy. Further, globalization is making criminal investigations and prosecutions increasingly difficult because, typically, several countries with different and often incompatible legal systems are involved.

Development of New Tools

Only a relatively small number of people have the necessary skills to attack ICT systems. However, once attackers find a particular vulnerability that can be exploited, they often write a software program to automate the exploitation of that vulnerability and make their program available for downloading on the Internet. Thus, every Internet user regardless of their skills has access to a range of software programs that can be used against various ICT systems.

2.4: Security Domains

Computer security is also frequently defined in terms of several interdependent domains that roughly map to specific departments and job titles within computer security. These

domains include; physical security, operational or procedural security, personnel security, system security and network security.

Physical security involves the controlling the comings and goings of people and materials; protection against the elements and natural disasters. Operational/procedural security covers everything from managerial policy decisions to reporting hierarchies. Personnel security involves hiring employees, background screening, training, security briefings, monitoring, and handling departures. System security is concerned with user access and authentication controls, assignment of privilege, maintaining file and file system integrity, backups, monitoring processes, log-keeping, and auditing, while Network security covers protecting network and telecommunications equipment, protecting network servers and transmissions, combating eavesdropping, controlling access from not trusted networks, firewalls, and detecting intrusions.

2.5: ICT security in institution of higher learning case of Georgetown University

Information and communication technology (ICT) is of strategic importance and essential functional requirements for many institutions of higher learning. All over the world, ICT is achieving a breakthrough in management and teaching of online learning, which helps to cater for the increased student population. However the security of the information being processed, stored and exchanged is a growing concern to the management as the dependence on ICT for most of the institutions' core services functions is increasing.

Institutions of higher learning are at a great risk because of multiple users and a vast amount of data ripe for threats internally and externally.

For the case of Georgetown University, they have a body called University Information Service Office (UISO). This office Committed to providing information, resources and tools in IT security for the Georgetown University community and alliances. It security plans include;

Focusing on information security and Electronic Protected Information (ePI), also known as legally protected information such as financial information, password, student records Encourages users to identify work PCs and laptops as dedicated work spaces, not for personal use

2.6: Challenges of ICT Security in Higher Education

In business domain, the concepts of guarding trade secrets, protecting corporate data from competitors, and fighting patent infringements are well understood. These types of information security have a strong history in industries such as manufacturing and music, where patent and copyright infringements could destroy the viability of the organization. In domains where information security has a strong history, every member of the organization is sensitized to critical security issues and views information security as a pivotal element for the organization's survival. The practice of safeguarding corporate information is reinforced by practically all activities of the enterprise.

Not all industries are adept at protecting information. Even in domains where regulations mandate information security, such as health care, applying sufficient resources to meet the mandates is difficult. Studies report that hospitals and medical facilities, for example, often fail to meet security requirements within the mandated time.¹

Information security is even more problematic in higher education. The underlying values and vision of higher education call for sharing knowledge and providing access to information and technology. In other words, the concept of information security runs counter to the open culture of information sharing—a deeply held value in academe.

This phenomenon is not unique to information security. The tension of “the acropolis versus the agora” is recognized in the management of higher education. To ameliorate this challenge, we must look for creative ways to segregate university information systems into two major categories:

- the academic systems for which the faculty want to maintain open accessibility, and
- The enterprise systems where legal compliance, data confidentiality, and data security are paramount, rather than information sharing.

Beyond the cultural tension are other challenges inherent to information security. First, information security can be categorized as a hygiene factor rather than a satisfier. When a robust system functions properly, safeguarding critical and confidential data, it is not obvious to many people in an organization, with the exception of the few individuals who work with the system on a daily basis. In fact, the average user may never know that a system is secure. The absence of a secure system could be experienced by many users, however, usually after damage has been inflicted on the system and it is too late to avoid the impact.

The second challenge is the perception of many people that data security is a technical issue and, therefore, the sole responsibility of chief information officers (CIOs) and their

staffs. This implies that as long as the CIO procures and installs the latest firewalls and other technical gadgetry, the system is protected. Such forms of myopic self-exoneration can exacerbate today's cycle of ever-increasing information security crises. Many authors have shown that technology alone is not the solution, that information security must be addressed by a combination of technical and administrative practices such as promulgating sound policies and implementing systematic processes to safeguard institutional data.

The third major challenge is the non-intuitive nature of information security and its adverse impact on productivity. The ease and low cost of collecting, storing, and sharing large volumes of information motivate us to assemble data at a continually faster rate and provide greater access to that data. Consequently, many view the steps that enhance security as a nuisance at best or a major impediment to improving productivity at worst.

Finally, another major misconception is that a single perfect solution exists to information security—that once this solution is implemented, the task of protection is complete. In reality, no single solution can address the information security requirements of an organization. Continual vigilance and ongoing effort are required because the job will never be done.

2.7: ICT security in developing countries the case of Tanzania

The significant achievement of ICT in Tanzania can be traced from early nineties after various adjustments in policy, regulatory and commercial facets, both macroeconomic and within ICT's converging sectors (Bakari et al, 2004). Since then, Tanzania has experienced dramatic changes in the use of ICT, coupled with limited knowledge, use of

different software and hardware imported from different places of the world, poor communication and power infrastructure and poor control and maintenance of the ICT in general. Significant developments can be traced from 1994 when the first TV station started broadcasting, with the establishment of mobile phone companies in 1995, and when Tanzania was connected to the Internet for the first time in 1996

Presently, Tanzania has a national ICT policy which is in place. Though it is in place many organizations currently are still struggling to come up with their own usage policy on how to handle and use organization's ICT assets and resources. Several trends in ICT are identified, including the rapid diffusion and dependence on ICT in many organizations, which have brought challenges and raised doubt as to the sustainability of the application of ICT in fulfilling organizations' objectives. For example: it is now becoming common to walk into an office for a particular service just to be told that the service is not available because the system is down due to a virus; there are no services available at the bank for some hours because there is some problems in the system; the salary will be delayed because there are some problems in the system, etc.

These trends showed deficiencies in ICT legal framework, harmonized security and systems standards, lack of appropriate knowledge (users, planners, managers and among suppliers) and general stakeholder security awareness. Observations made in various papers in the introduction have indicated some degree of vulnerability of the implemented systems and some have gone further by giving highlights of the security problems in general.

2.8: ICT security management in non-commercial organizations

Non-commercial organizations are organizations that are not profit making but have non-financial objectives and goals to achieve. Such organizations include government institutions like public universities, public healthcare, etc. ICT security management is a combination of several aspects involving policies, standards, guidelines, codes-of-practice, technology, human issues, legal and ethical issues [Eloff & Eloff, 2003]. A comprehensive Information Security Programme contains a proper balance between people, processes and technology to effectively manage risks with minimal impact on the organization's operations. According to [Bishop, 2003], human beings are the weakest link in the security mechanisms of any system. Human issues may be divided into first, organizational problems which are lack of resources, lack of trained people and the tendency to consider security issues as secondary ones; secondly people problems grouped into insiders and outsiders.

While in commercial organizations the main objective is to hedge shareholder value, in non-commercial organizations the main objective is to meet the organization's missions such as business continuity, deliver quality services, minimize business interruption, eliminate fraud and corruption, minimize loss of property, protect copyright, ensure privacy, ensure confidentiality and minimize consequential liabilities, protect organization's reputation, etc. The ability of any organization to achieve its mission and meet its business objectives is directly linked to the state of its computing infrastructure. Although in non-commercial organizations the objective is not to make profit, risks associated with ICT use do have financial implications too. Therefore, in order to ensure

that, the non-commercial organizations meet their objectives, there must be an insurance structure which encompasses insurance policies such as ICT security policies, standards, guidelines, codes-of-practices, technologies, legal and ethical issues to counter the risks associated with ICT.

When a commercial organization makes a loss, one can make decisions on business grounds such as closing the company, etc. However, one cannot close the non-commercial organization like a public university or a government ministry for the loss associated with the ICT risks. One of the measures one can take is to estimate the loss on the one hand, which in most cases might be associated with the cost of reactivating the affected services. On the other hand, one can estimate the loss by also associating it with the cost of putting the service right so that that particular problem does not happen again. Finally, and which is more challenging, is working out the estimates associated with those who are affected by the absence of the system/system malfunction. Most non-commercial organizations have become increasingly dependent on highly complex and heterogeneous ICT platforms, and hence more exposed to ICT related risks [Magnusson, 1999]. If these risks are not taken care of, the objectives of these organizations will be affected negatively.

2.9: Conclusion

In this chapter, the researcher has reviewed several literatures and articles related to ICT security. ICT security goes beyond the three commonly known pillars of Confidentiality, Integrity and Availability. Other important factors include Accountability, Authenticity,

Privacy and Non-repudiation. Other areas covered include managing ICT security in non-commercial organizations, institutions and in developing countries with a focus on Tanzania.

Generally from all the reviewed materials, its clear that ICT security is vital in securing ICT assets, strategic information of the organizations and ensuring continuity of any organization.

CHAPTER THREE: METHODOLOGY

3.0: Introduction

The rationale of the study is to get the actual current situation on computer and information security in KIU, weighing if current measures are adequate and effective i.e. measuring up to the desirable ICT security requirements, if they have not then the problem should be identified and then a possible solution provided.

3.1: Study Area

The study was conducted at Kampala International University main campus located in Kansanga, Kampala Uganda.

3.2: Description of the study population

The study population consisted of members of staff of Kampala International University from different faculties and departments.

3.3: Research design

In carrying out the study, the researcher employed descriptive survey design of which it mainly used a qualitative approach but also with some aspect of quantitative research design. This design was chosen because the study was to get people's views and opinions on ICT security.

3.4: Methods of Data Collection

Data was obtained using different instruments/ methods. Interviews, questionnaire and observation were the main methods used. All these methods were used so as to complement each other and to validate the data collected.

3.4.1: Interviews

- i. The researcher carried out interviews in all the necessary departments but mainly focused on the ICT department. The interview was structured in that, and the questions asked were pre-planned and written in advance by the researcher. In a few instances extra questions outside the pre planned ones were asked especially in cases where it deemed necessary in getting more information.

3.4.2: Observation

The researcher used this method since he is already a staff member of the University. Since the study is on security of ICT systems, observation of the systems yielded good outcome

Observation was used for the following because it helped in checking the validity of data obtained through other methods. This was good increasing reliability of the data/information gathered. The researcher was able to see exactly what was going on and though observation, the researcher could see what was missing or inaccurately described

by other fact finding techniques. Observation was relatively inexpensive compared with other fact-finding techniques.

3.4.3: Questionnaires

The researcher distributed fifty questionnaires to supplement the information gathered using interviews and also to those who were not readily available for interviews, due to their job schedules or other reasons.

This method was especially useful in cases where the respondents were not comfortable giving their views or answers using interviews.

3.5: Data analysis method

In analyzing the quantitative data collected, the researcher used the Microsoft office Excel. For the qualitative data collected which were based on opinions expressed by the respondents were analyzed by a statistical method developed by the researcher in relation to already existing facts in order to arrive to a conclusive result.

CHAPTER FOUR: FINDINGS AND ANALYSIS

4.0: Overview

This chapter presents the findings after analyzing the questionnaires and interview. It shows the response got out of the study carried out to gain insight on the state of ICT security in KIU.

4.1: Data analysis

This section presents analysis as reflected by the responses got from the questionnaires which were supplied to the members of staff from different departments and faculties/schools of KIU. The questionnaires were aimed at addressing the following; firstly to establish the current state of ICT security of KIU. Secondly, was to get the effects of ICT security and finally, to help in improving the state of ICT security management in Kampala International University.

The findings were a reflection of what is on the ground concerning the subject. These findings applied to the sample and gave a reflection of the total population from which they were drawn.

4.2: Population of the study

There were a total of 50 respondents. These` respondents in the study were drawn from the following departments and faculties

- i. School of Computer Studies
- ii. School of Business and Management
- iii. Faculty of Education

- iv. Faculty of Law
- v. Faculty of Social Sciences
- vi. Institute of Distance Learning
- vii. Department of Finance
- viii. Department of Admission
- ix. Human Resource Department
- x. Directorate of Student Affairs
- xi. Directorate of Academic Affairs
- xii. School of Post Graduate Studies
- xiii. ICT department and the
- xiv. Library

These respondents were university staff including, faculty/School administrators, administrative secretaries, clerks, lecturers, departmental heads, course coordinators and examination officers. There were at least two respondents from each department / faculty with school of computer studies and department of ICT having a little bit more respondents than the rest.

4.3: Results and Analysis of Findings

The researcher found out the following in the research.

4.3.1: ICT facilities available

The ICT facilities which were being considered included; computers, printers, scanners, internet, photocopiers, computer networks among others. The respondents identified several ICT facilities in their various departments. At least each respondent said that they

had a computer and most of them had printers. Many respondents who said to have computer networks also reported to have internet, although the internet was not reliable enough in that half of the time it was not there. Photocopiers and scanners seemed to be scarce.

4.3.2: Management of ICT Facilities (Security Management)

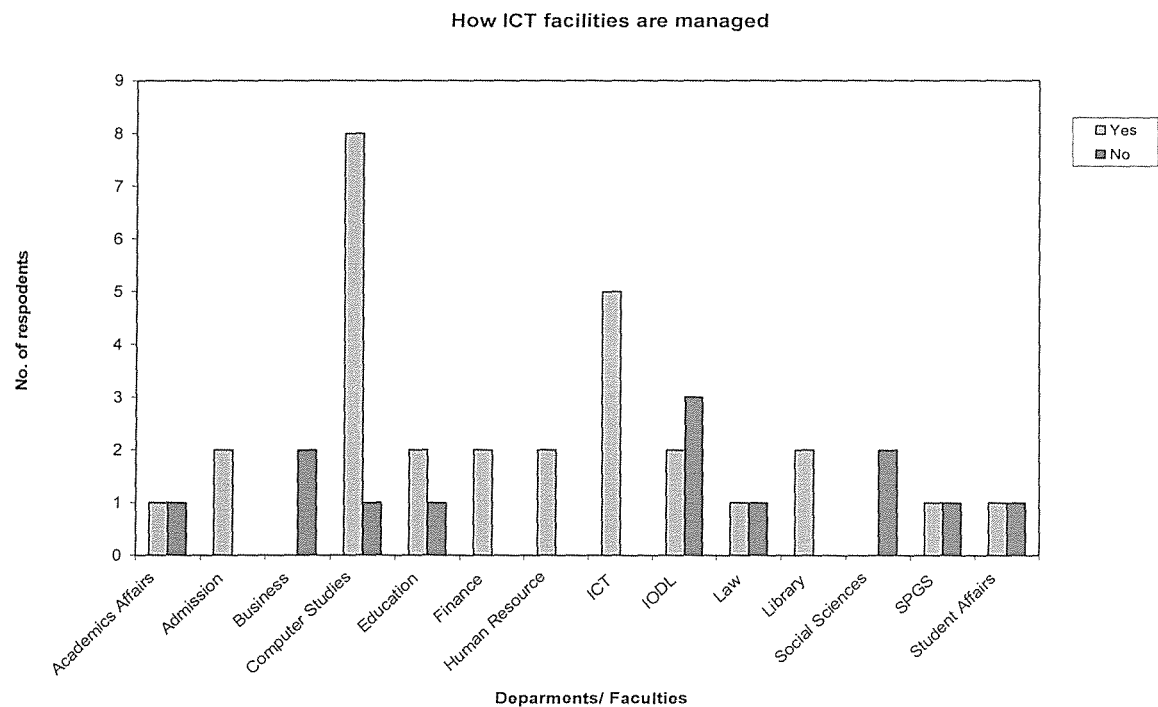


Figure 2: Response on whether there is someone in charge of ICT security within departments

The results above, showed that in majority of the department and faculties there was someone in charge of ensuring that the ICT facilities were secure. It was only in the faculties of business and social sciences where the respondents said that no one was in-charge of ensuring ICT security.

The overall response on management ICT security was as follows.

Response on management of ICT facilities

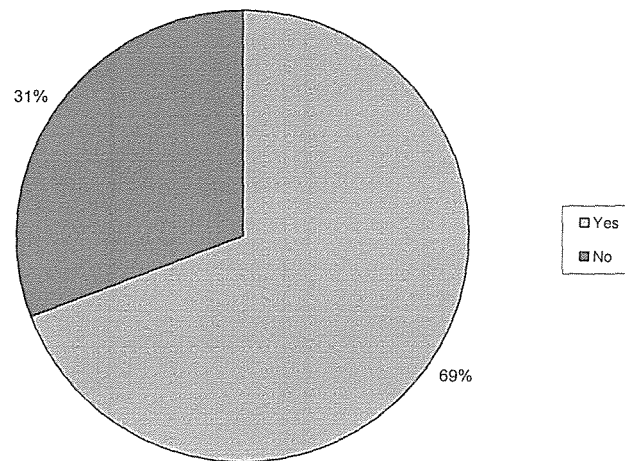


Figure 3: Overall response on whether there is some in charge of ICT security management

The figure above shows that almost 70% of respondents agreed that someone is there to ensure security of ICT facilities.

4.3.3: Use of password as the access control mechanism

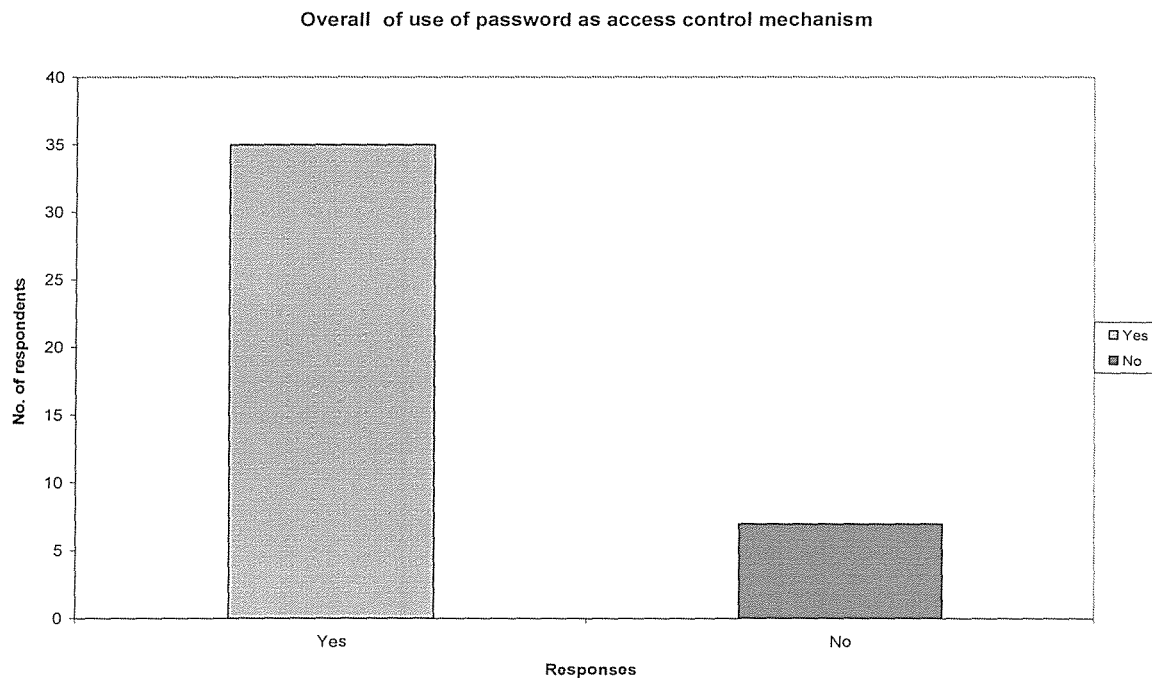


Figure 4: Response of use of password as an access control mechanism.

Most respondents agreed that the main mode of access control to computers was by use of password. The few who disagreed indicated that no other access control was in use; instead, the machines were open to anyone for access. The analysis is indicated by the pie chart below

Password as the access control mechanism

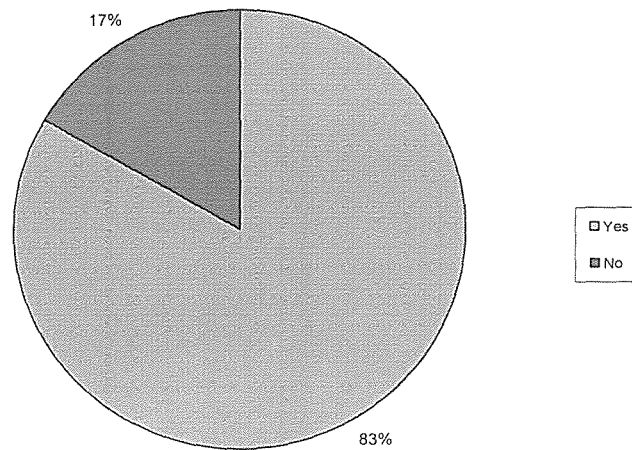


Figure 5: Analysis of passwords as access control mechanism

4.3.4: Protection against viruses

Three aspects were addressed in regard to computer protection against viruses. These were, installation of antivirus software on machines, updating the antivirus and the frequency of virus scan on machines. The results were as follows;

Installation of antivirus software:-

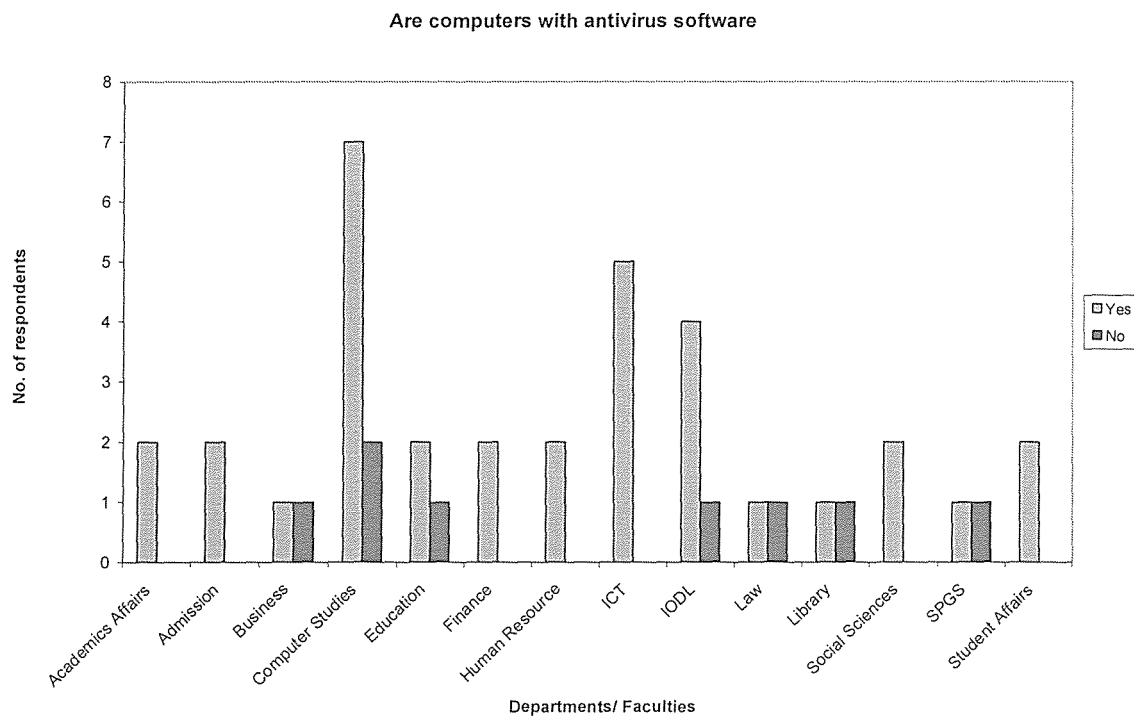


Figure 6: Departmental response on antivirus update

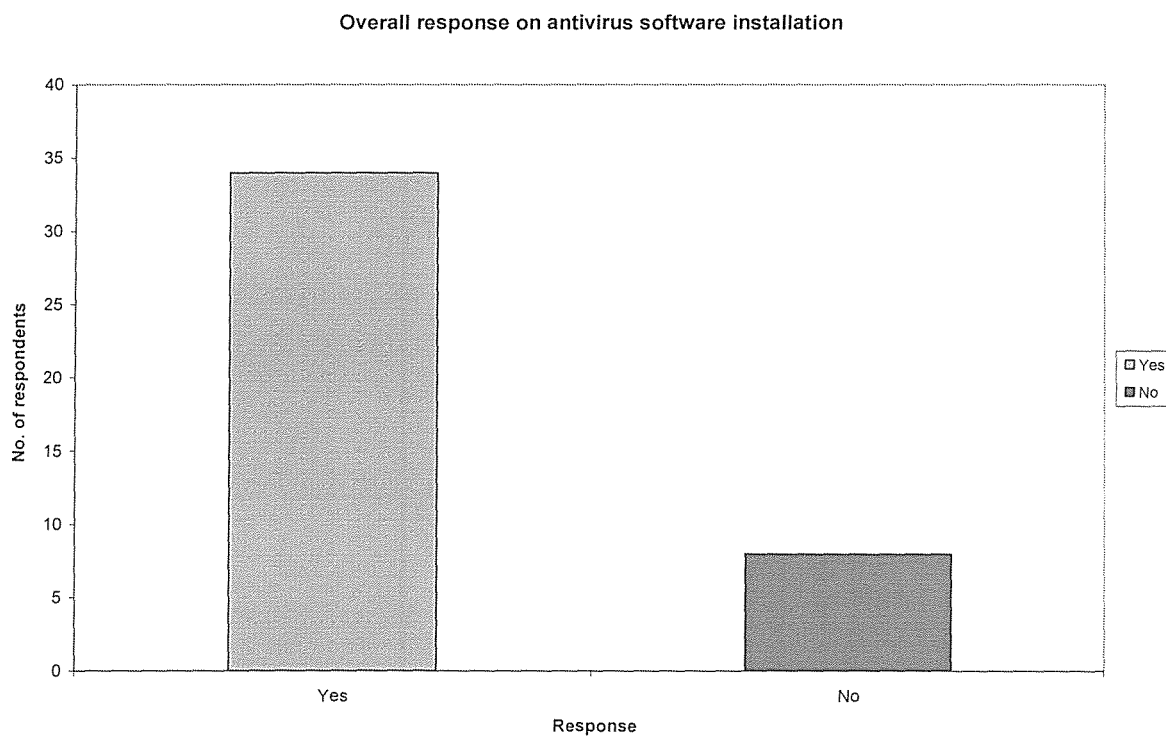


Figure 7: General response on installation of antivirus on computers

The findings showed that majority of the respondents represented by 81% said that many computers were installed antivirus software.

Updating of antivirus:-

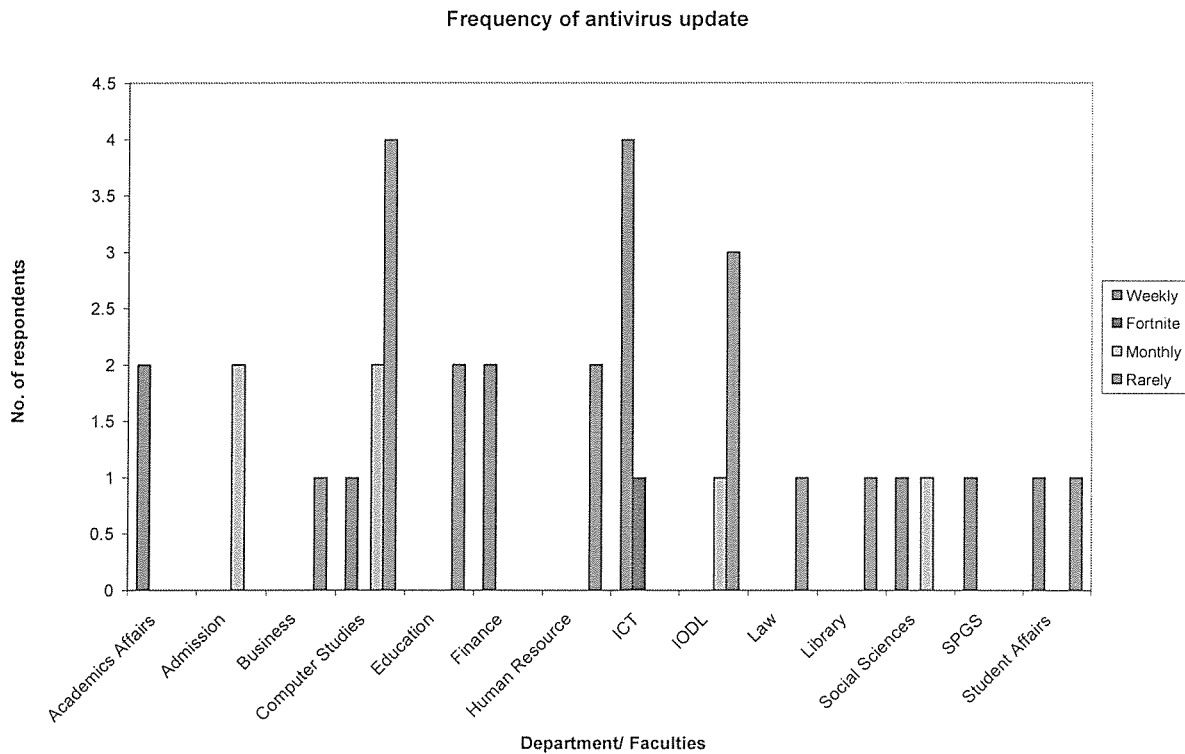


Figure 8: Frequency of antivirus update in different departments.

The above findings indicates that only in ICT department, does the update of antivirus done frequently otherwise most respondents indicated that antivirus update is done rarely. This is clearly seen in the overall or general picture painted by the respondents in the figure below

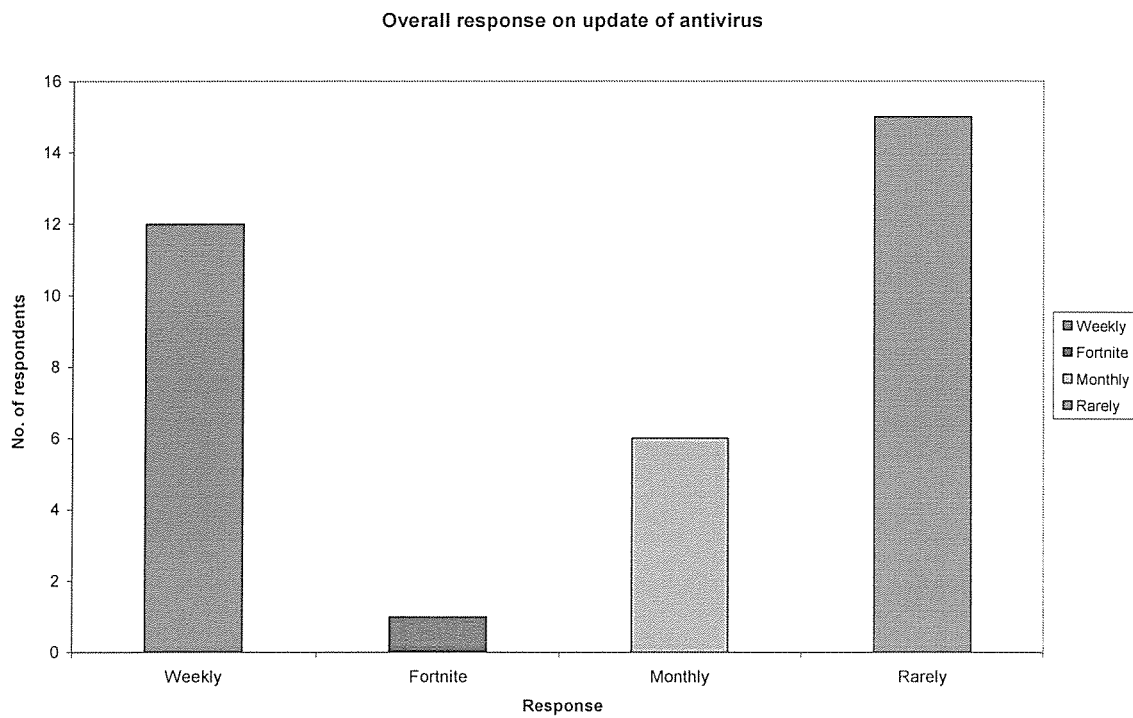


Figure 9: general response on antivirus of antivirus

About 65% of the respondents acknowledged that it takes more than a week to update the antivirus.

Frequency of virus scan:-

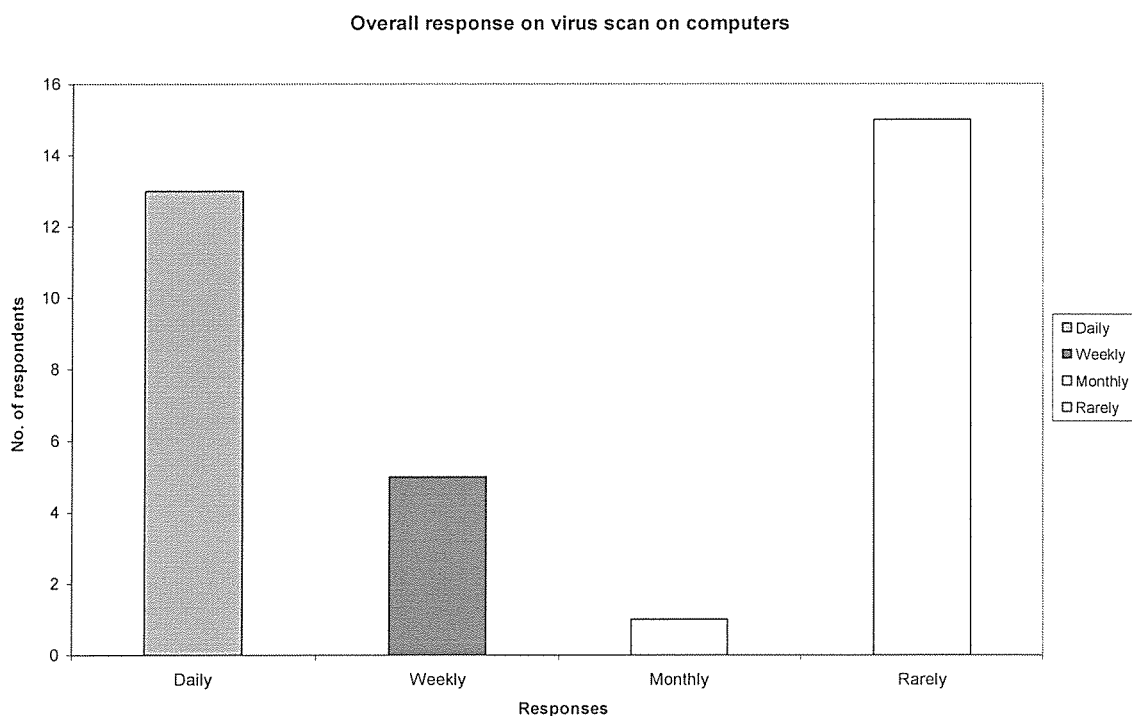


Figure 10: Frequency of virus scan according to respondents

These findings show that more respondents said those virus scans were done rarely compared to others. But overall, there were a little bit more than half i.e. 56% of the respondents who indicated that virus scan is done daily or weekly as shown by the pie chart below.

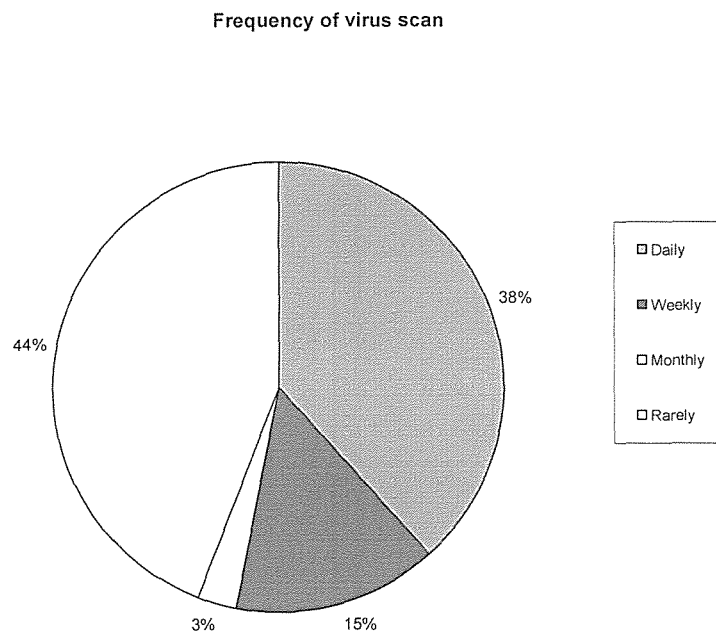


Figure 11: Analysis of the general response on virus scan

4.3.5: Maintenance of ICT facilities

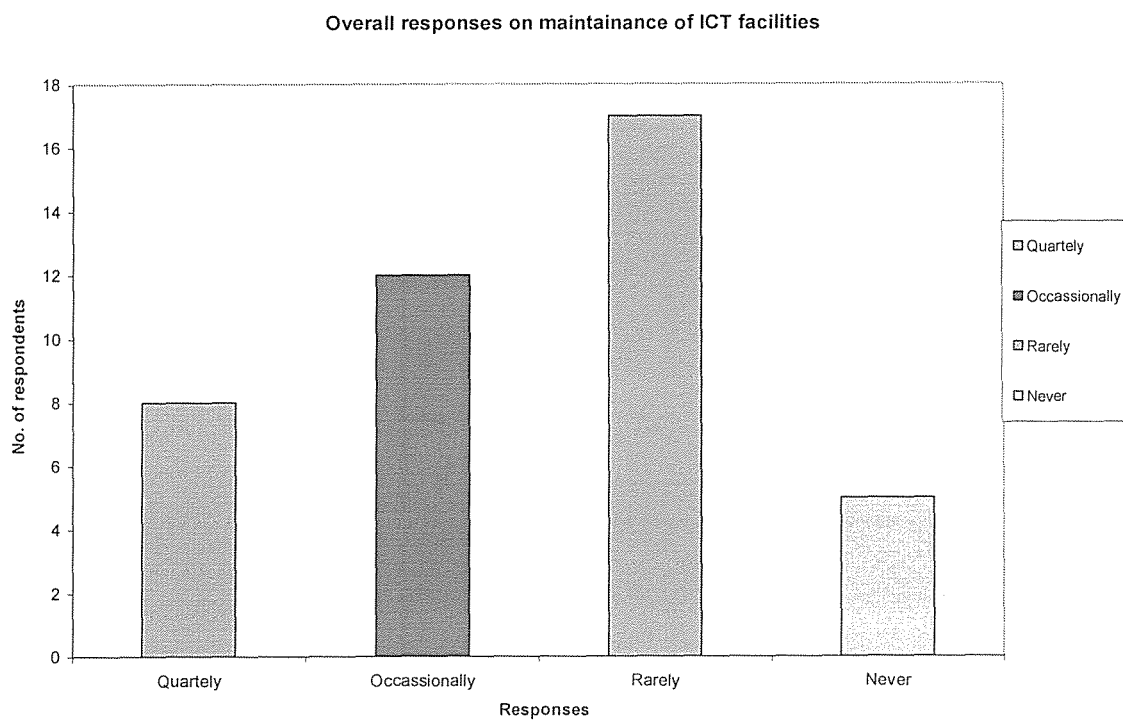


Figure 12: Response on frequency of ICT facilities maintenance

The results from the respondents show that maintenance of ICT facilities is rarely done.

In fact one of the respondents said that it is done only when these facilities are down.

After analysis of these using a pie chart shows the following results;

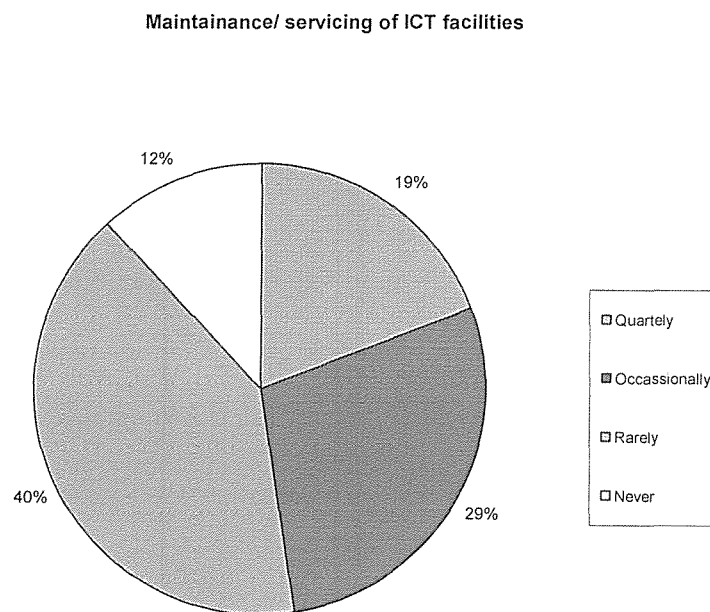


Figure 13: analysis of response on maintenance of ICT facilities

4.3.6: Data backup

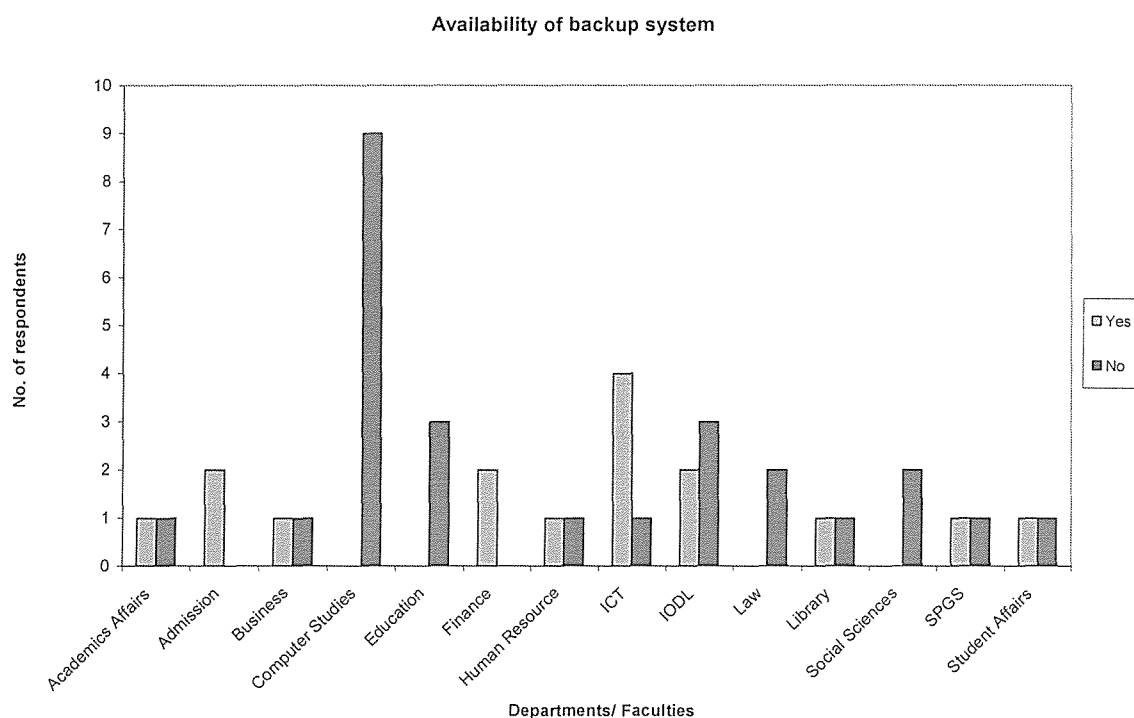


Figure 14: Response on availability of back up mechanism according to departments

Figure 14 above shows that according to the response given backing up of data is not a common thing. Only of a few departments notably admissions, finance and ICT of have mechanism of backing up their data. This analysis is worse even more when depicted using a pie chart.

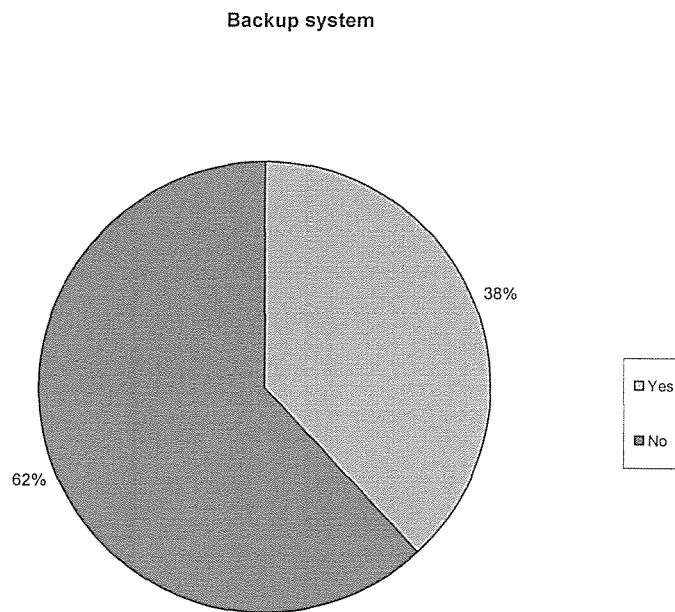


Figure 15: An overall analysis of availability of data backup mechanism

Frequency of data backup:-

Among those departments and faculties which reported to have some form of data backup mechanism a further enquiry was carried to see how frequent is the data backup done.

The figure below shows the frequency.

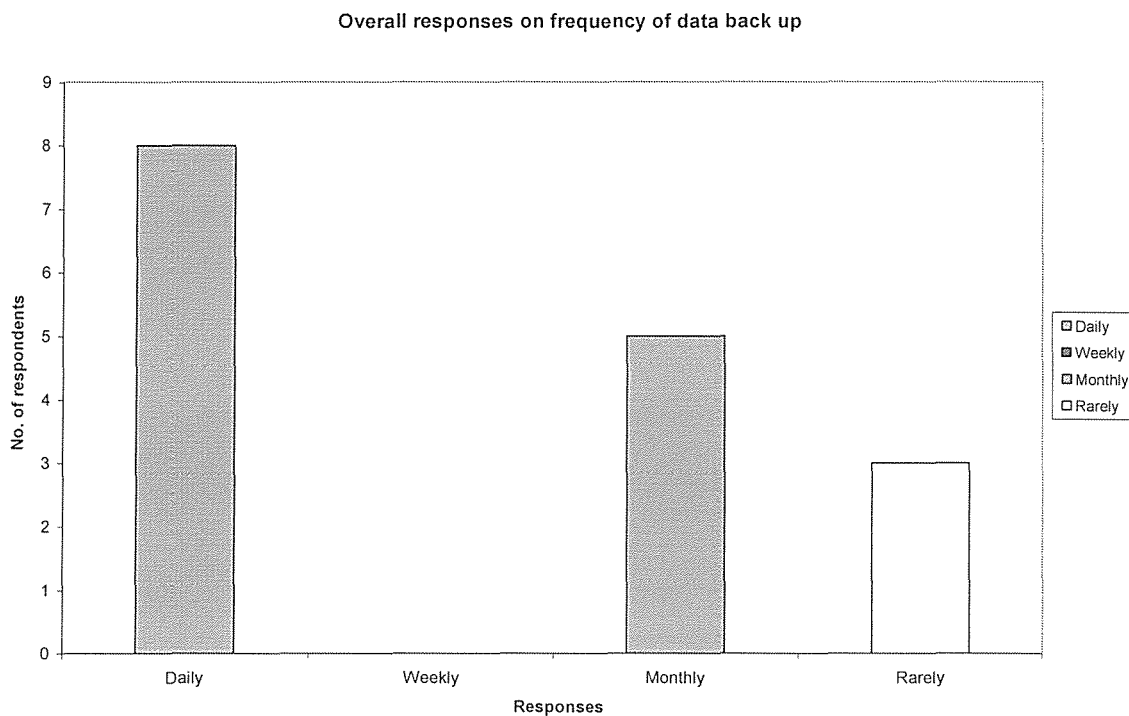


Figure 16: An analysis of data backup frequency

The above findings indicate that data backup is done on a regular basis among the departments who do so.

4.3.7: ICT security measures

The researcher needed to know if there were any measures in place instituted to ensure that ICT security e.g. any ICT security policy or ICT policy in general. From the general response from the respondents, the indication showed as shown below.

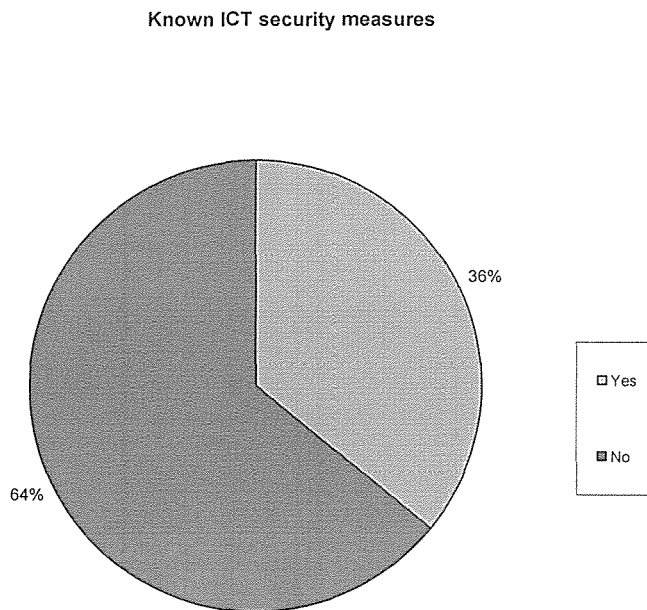


Figure 17: Pie chart showing respondents knowledge existence of any ICT security measures.

The 36%, who agreed that there were some measures, were mostly from ICT department. The researcher was informed that there was an ICT policy in place but this information was not known by many. This was further seen by analysis of how readily available the information was as depicted by the respondents who acknowledged the availability of the measures. Only less than 35% said it was readily available.

4.4: Improvement of ICT security

The researcher went ahead to inquire the respondents on what they felt needed to be improved concerning ICT security or what they wanted to be introduced to ensure the same. There were several things which they said if improved or implemented the security of ICT will be enhanced. Some of the things suggested include:

- a. Availability of reliable internet. The respondents said that internet access was vital especially for automatic update of the antivirus. The current internet service was said to be unreliable in that it is on and off. Moreover the internet was said to be very slow especially during the day yet those are the working hours.
- b. Employment of ICT security officers. It was noted that the within ICT department , there is need of personnel dedicated to ensuring that information secure the institution has done a lot to ensure physical security, by having security guards and putting up measures to avoid theft of IT facilities. On the other hand, little has been done on information security.

4.4: Current ICT security issues

From the responses given by the respondents and through observation, there were several ICT security issues which the researcher noted. These issues both directly and indirectly affect ICT security.

4.4.1: Viruses, worms and Trojans.

A virus is a computer program that can copy itself and infects computer without the permission or knowledge of the owner (Businge, 2009). Though the term virus is commonly used to refer to any spy ware program, ad ware and mal ware programs, not all these types of programs have the reproductive ability. A worm is software program capable of reproducing itself that can spread from one computer to the next over a network where as a Trojan horse or simply a Trojan is a program that appears harmless and genuine but has hidden agenda which is destructive.

Viruses, worms and Trojan horses are common security threat in most computer systems in KIU and statistics shows that at least 80% of the computer systems are 'infected'. These viruses are got the internet and use of external storage devices which are infected. Although most systems are installed with antivirus soft wares, most of the time they are not kept up to date on virus definitions. This renders these antivirus soft wares useless.

4.4.2: System crash

A system is said to have crashed in the event that a computer becomes in operative. i.e. the computer fails to respond to commands. In many instances the computer systems displays a blue screen. From the interviews carried out by the researcher it emerged that there are several instances whereby there has been a system crash. At least in all the departments they reported cases of one or two computer systems crashing.

4.4.3: Data back up

Backing up of data is storage of files in an offsite location for safety purposes. The research revealed a poor culture of backing up files within KIU. More over there is no systematic way of doing it.

4.4.4: Use of pirated software

The research also revealed that more than 90% of the soft wares used in Kampala international University main campus are pirated i.e. they are not original or genuine. In effect this has led to system crash and loss of data and information.

4.5: SWOT analysis of management of ICT security in KIU

The researcher was able to get quite enough information about ICT security in KIU. After analyzing, the researcher used the Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis method to identify and present the achievements and areas which need improvement. This is represented on the figure below

Strengths <ul style="list-style-type: none">○ The institution has staff members who are committed to ensuring that information security is enhanced○ The existence of ICT department mandated with management and control of ICT services and facilities in the university.	Weaknesses <ul style="list-style-type: none">○ There is lack of enough sensitization among the students and the whole KIU community at large on institution's policies○ Goodwill from the management is not really seen especially in terms of funding for the acquisition of some of these ICT facilities and employment of human resource○ There is lack of proper guidelines towards ensuring ICT security○ The institution is not so keen in staffing the department of ICT
Opportunities <ul style="list-style-type: none">○ The availability of internet services in	Threats <ul style="list-style-type: none">○ The institution does not have a clear

<p>the institution can be used to enhance and improve ICT security e.g. in getting updates on virus definitions</p> <ul style="list-style-type: none"> ○ The availability of ICT specialist in the institution. This includes the IT lecturers who can contribute ideas towards better and achievable security measures ○ Embracing newer and more efficient access control mechanisms instead of passwords only 	<p>policy concerning ICT nor clear guidelines towards appropriate use of ICT facilities</p> <ul style="list-style-type: none"> ○ Lack of coordination on management of security between the ICT department and other departments ○ Unreliable power supply. This affects the ICT systems in place and also the facilities. This can have adverse effects on the services being offered by the institution
--	---

Table 1: SWOT Analysis table for KIU ICT security

CHAPTER FIVE: DISCUSSION, RECOMMENDATIONS AND CONCLUSION

5.0: Overview

In this chapter the researcher discusses the study, brings out some recommendations and concludes the study. The researcher also points out areas of future research. It contains subsections 5.1 presenting the discussion, 5.2 presenting the researchers contribution to the study, 5.3 containing the conclusion and sub section 5.4 suggesting some of the possible future areas of research.

5.1: Discussion

The research found out several things concerning ICT security in general and more particularly on Information and information systems security. As earlier mentioned ICT security is vital for any institution and in that sense Kampala International University is not left out. Its importance cuts across every department within the university as expressed by the respondents in the research.

Though ICT security is important, majority of the people do think that it has not been properly addressed. There are no clear guidelines on it. Virtually individuals have to come up with their owned ways of providing security to their systems. In most instances the methods employed are below standard.

In order to protect any information, access control mechanisms needs to be employed. The research found that many people employ it as quite a big percentage of over 80%

used passwords to protect system access. Unfortunately no other access control mechanism was being used

On the issue of maintenance of ICT systems, virtually none is done apart from when theirs is a breakdown or system crashing. The frequency of maintenance needs to be improved such that it is done on regular basis.

From observation it was noted that physical security to ICT hardware facilities is well taken care of. Security guards are well deployed thus guarding against intrusion. In spite of this, the researcher thinks that sensitive areas with critical ICT facilities and information security should be improved beyond only having security guards.

One of the main threats to information as noted by the researcher was the issue of viruses, worms and Trojans. Majority knows of their effects on systems but ensuring a virus free environment is a big task, this is because as much as many computers are installed with antivirus software, ensuring that these software are regularly updated has not been achieved.

The researcher also found out that the idea of backing up data had not been well embraced as majority of the departments did not perform back up of data. Moreover where data back up was done, the method used and the frequency of doing it needed to be improved. incase of any disaster occurring which may lead to loss of data, the researcher

established data the contingency measures in place in order to ensure that there is continuity are somehow weak.

Through out the research it was established KIU was an already existing ICT policy document developed about two years ago. In it, policies concerning ICT security and usage are elaborate. But its existence and the content are barely known to the public, this is because no sensitization has been done. Moreover, the implementation part of it has not yet been done. Mainly those who know about it are the a few staff within ICT department. Those it only remains to be a document.

5.2: Recommendations

The questionnaires and interviews conducted including observation made during the research led to the establishment of challenges facing ICT security in Kampala International University. Therefore the researcher has come up with a proposed framework to help the institution be able to secure its ICT facilities and services more efficiently. This framework reflects the challenges and how they can be minimized.

5.2.1: Proposed framework for ICT security for Kampala International University

The proposed framework for ICT security for Kampala International University was developed by the researcher in a bid if adopted help in improving the current state of ICT security management by the institution. It highlights some of the major issues which need to be addressed and some of the ways of ensuring efficiency in provision of security.

The issues of ICT security ought to be taken seriously by the institution and this can be done by

Goodwill from the management

The support from the managerial organ of the institution is very important. Realizing the importance of securing ICT facilities and services to the well being of the institution and its continuity, the management should be in the forefront of ensuring ICT security is efficiently managed. They should readily provide any support needed by the ICT directorate of the institution concerning the security issues, these includes setting aside certain amount of funds towards the same on every budget calendar of the university. Also providing advices and listening to advices given by the ICT directorate towards security enhancement. The management needs also to participate in an awareness campaign of ICT security importance among the KIU community, and any other way the can.

Skilled personnel

The directorate of ICT is a body of KIU mandated with the task of managing and monitoring all ICT related issues within the institution. However the skilled personnel they have is not enough to ensure ICT facilities and services are secure in all the areas of the university. With liaison and advice from the directorate of Human Resource of KIU, ICT directorate should get enough skilled personnel at least every department/ faculty of the institution should have ICT personnel in charge of securing ICT facilities and services within that area.

Also in general the ICT directorate should employ a staff specialized in ICT security to be in charge of overseeing ICT security within the institution. This person shall be the ICT security administrator. This administrator shall be responsible of coming up with appropriate ICT security measures for the university and shall be working closely with the departmental ICT staff to ensure that these measures and other ICT guidelines are adhered to.

Awareness KIU ICT policy

The research revealed that very few people within the university have the knowledge of existence of an ICT policy for the university called “Kampala International University ICT Policy 1st Draft”. Though it is in draft form, its awareness among the university community is important. An awareness campaigns should be carried out as this will enable the community to know about the IC T regulations and guidelines of which it will also help in ICT security. Also fast tracking the implementation of the policy by the management is critical.

Usage of ICT facilities and services

Not everyone within the university have adequate knowledge on the ethical use of ICT facilities and services. There is need of sensitization of the users on the acceptable manner of using the facilities and services as provided within the institutions regulations and guidelines.

Appropriate use of ICT services and facilities is critical as some of the users abuse or misuse these services and facilities without knowing, given that these are regulations which may not be universal.

Training, seminars and workshops

Modes of administering ICT security are ever changing as the challenges towards the same also increase. Newer security challenges on ICT keep emerging and they require newer approach of which they cannot only be tackled on a general way. The need for regular training, seminars and workshops for ICT staff members the university community is therefore important. Through these trainings, seminars and workshops the staff gets to be informed on emerging technologies and measures of ensuring efficiency in ICT security.

The trainings can be locally arranged by the ICT directorate or from other ICT service providers. Local trainings may also include even other ICT users within the university. For these to be successful all the necessary stakeholders need to participate and the facilitation of the trainings.

Physical security

Securing the physical location of ICT facilities and services is important. Currently the institution uses security guards to provide physical security. This may not be enough and the use of automated systems is better. This is so since automated security systems are not bound to human weakness like tiredness.

Automatic burglarproof systems should be installed in offices to enhance the security. These systems provide better security services which will not only be beneficial for ICT facilities and services but even for other facilities as well. These systems are especially critical for rooms which are very sensitive like ICT office, data bank examination room, computer labs etc.

Access controls mechanisms

Access controls mechanisms implies the methods used to ensure that only authorized personnel are the ones who gain access or have the authority use certain ICT facilities and or services. Efficient access controls mechanisms should be used right from accessing of offices and rooms, ICT facilities and even ICT services.

Currently the main access control mechanism employed is the use of passwords in accessing computer systems and databases (information). This controls access to facilities and services only. Furthermore, the way this mechanism is administered is not ensure maximum security since majority of users share their passwords and the way of coming up with them is poor. Majority of the passwords can be hacked into. A guideline on the use of passwords should be developed. This will help on how to come up with password and renewing or changing the passwords.

Another access control mechanism which should be considered is the use of biometrics. Voice detection systems and/or fingerprints systems can be embraced. Such systems can be installed on rooms like server rooms and data banks. These systems will not only

prevent unauthorized access but also it is easy to track users bus use of the access logs recorded by the system incases of security breach.

Backup systems and contingency plans

ICT systems like all other systems are prone to suffer from disasters or any unforeseen tragedies. Therefore, backup systems should be in place for information. Backing up of data is where data is duplicated on another place to ensure in case of any tragedy like system crash one can still access information.

The directorate of ICT should establish or come up with an offsite place where institutions data can be backed up and also provide guidelines on how it should be done. Also real-time automatic back up of data is advised.

On contingency plans should be put in place of ensuring that incase of misfortunes daily operations of various departments are not interrupted. Again the directorate of ICT in liaison with other department can come up with necessary measure to ensure this is achieved

Software packages

The software packages to be used within the institution's computers needs to be valid and genuine. Genuine software packages are of good quality and are durable. This will reduce on cases of unexplained data loss and system crash. This will ensure availability and integrity of information.

Antivirus installation and updates

All the computer systems belonging to the university and those which access the university network need to have antivirus software installed in them. The ICT directorate of the university needs to enact guidelines on installation of this software and its update.

It will be necessary to get licensed antivirus software from a reputable company. The antivirus should be able to be updated automatically online. Also daily or regular virus scans should be carried out. The users need to be sensitized on the importance of doing so.

5.3: Conclusion

The research conducted has revealed a lot concerning ICT security management in KIU. It has revealed the current state of ICT security by bringing out how it is being managed and also what is currently in place.

By showing as is in place the research has highlighted on both the weakness and the strength in KIU's ICT security. This has led to the researcher coming up with recommendations in form of a framework.

The institution can be able to use the framework to come up with an elaborate ICT security policy for the university. This will be achieved by improving of the framework and probably carrying out a wider consultation with ICT security experts

5.4: Future research

ICT security is a very wide field of study. This research focused mainly on ICT security on facilities and services. The framework developed from the research can serve and be of great importance to the university. However, related areas where further research can be conducted include;

- Challenges in implementation of ICT policies within organizations
- Network security

5.5: Limitations of the research

The research was faced by a few hitches. This included difficulty in getting information. During data collection process, many people did not want to participate in the interviews and there were several questionnaires which were not returned.

The time for doing carrying out the research was also not adequate given that the research also works and creating extra time was not easy.

In some instances there were problems of power blackouts. These also contributed a lot negatively especially during data analysis and report writing

REFERENCES

1. Adam Shostack, Andrew Stewart, 2008, The New School of Information Security,
2. AHIMA, (2005). The State of HIPAA Privacy and Security Compliance.
Retrieved from
http://www.ahima.org/marketing/email_images/2005PrivacySecurity.pdf
3. Alec Yasinsac, (2002), Information Security Curricula in Computer Science Departments: Theory and Practice, Department of Computer Science Florida State University, Journal of Computer Security
4. Bakari Kuwe Jabiri (2007), A Holistic Approach for Managing ICT security in Non-Commercial Organizations. Retrieved from
www.humanit.org/PID/IPID%20workshop/Jabiri%20Kuwe%20Bakari.ppt
5. Bakari Jabiri Kuwe, Yngström Louise, Magnusson Christer, Chaula Job Asheri, Towards managing ICT security in non-commercial Organizations in developing countries, Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology
6. Businge Phelix Mbabazi, (2009), Fundamentals of ICT Introduction to Information Technology, 1st Edition, Matgeox Enterprises, Kampala Uganda.
7. Bishop Matt, "Computer Security, Art and Science" Addison Wesley, ISBN: 0-201-44099-7.
8. Courtney, R. (1977), Security risk analysis in electronic data processing", AFIPS Conference Proceedings NCC, *AFIPS Press*.
9. ICT Security. <http://www.uonbi.ac.ke/ICT/security.php>
10. ICT Security tips. http://www.utas.edu.au/itr/security/security_tips.html

<http://security.georgetown.edu>

11. Information Security Governance Assessment Tool,
<http://www.educause.edu/ir/library/pdf/SEC0421.pdf>
12. M.M Eloff & J.H.P Eloff, "Information Security Management – A new Paradigm:
Proceedings of SAICSIT 2003
13. J. J. Gonzalez, and A. Sawicka, (2002) "A Framework for Human Factors in
Information Security," paper presented at WSEAS International Conference on
Information Security, Rio de Janeiro. Retrieved from
<http://ikt.hia.no/josejg/Papers/A%20Framework%20for%20Human%20Factors%20in%20Information%20Security.pdf>
14. Magnusson Christer, "Hedging Shareholders Value in an IT dependent Business
Society" THE FRAMEWORK BRITS, Ph.D Thesis, Department of Computer
and Systems Science, University of Stockholm and the Royal Institute of
Technology, Stockholm, 1999, ISBN: 91-7265-011-7
15. Mohammad H. Qayoumi and Carol Woody, Addressing Information Security
Risks, Educause Library: Retrieved from
http://www.educause.edu/content.asp?page_id=5746
16. Kroenke, David (2008). Using MIS - 2nd Edition
17. Rockart et al (1996) Eight imperatives for the new IT organization Sloan
Management review
18. SIS. (2003), SIS Handbok 550. Terminologi för Informationssäkerhet." SIS
Förlag AB, Stockholm (in Swedish).

19. Swissinfo, 2003 "Language Gap Threatens Access to Information," Retrieved from <http://www.swissinfo.org>
20. O'brien James A. (2003). Introduction to Information Systems, essential for e-Business enterprise, 11th Edition, McGraw-Hill Irwin
21. Syngress 2007, The Best Damn IT Security Management Book Period,
22. Peltier, Thomas, R. 2002. "Information Security Fundamentals."
23. UNESCO, 2002. „Information and Communication Technology in Education – A Curriculum for Schools and Programme of Teacher Development“. *Division of Higher Education*, UNESCO, France. Retrieved 29 Sept. 2009 from <http://www.gocsi.com/ip.htm>
24. Information security Paper, 2006. Retrieved on 14th November 2009 from <http://www.businessdictionary.com/definition/information-security.html>
25. Information Security Management. Retrieved 14th November 2009 from <http://jobsearchtech.about.com/od/historyoftechindustry/g/InfoSecurity.htm>
26. Introduction to ICT Security. Retrieved 14th November 2009 from <http://www.albion.com/security/intro-4.html>

APPENDICES

APPENDIX A: Questionnaire:

AN ANALYSIS OF ICT SECURITY MANAGEMENT IN KAMPALA

INTERNATIONAL UNIVERSITY

Introduction

My name is Korir Amos Kipkosgei, a student of Master of Science in Information Systems at Kampala International University. I kindly do request you to answer the following questions as concerning my Research entitled “Analysis of ICT security management at Kampala International University”.

Confidentiality

The answers given to these questions will be treated with a lot of confidentiality and no part of the information given will be used outside the scope of the study

NB: Please fill in the blank spaces and tick in the correct boxes.

1. Which faculty/ department to you belong to?

.....

2. Which ICT facilities are available within you faculty?

☐

Computers

☐

Printers

☐

Internet services

☐

Scanners

☐

Photocopiers

☐

Computer network

☐

Others (Please list them).....

.....

3. Is the any one in charge of ensuring that these facilities are secure?

☐ Yes ☐ No

If Yes, who (give the title of the person).....

.....

If No, how is their security ensured?

.....

4. Is the access to computer systems by use of passwords?

☐ Yes ☐ No

If No, what security control mechanism do you use to keep your systems safe from unauthorized users?

.....

.....

5. Are the computers installed with antivirus software?

☐ Yes ☐ No

If yes, how often is the antivirus updated

☐ Weekly ☐ After every two weeks

☐ Monthly

☐ Rarely

How often are your computers scanned for viruses?

☐ Daily

☐ Weekly

☐ Monthly

☐ Rarely

6. How often are the ICT facilities serviced?

☐ After every three months

☐ Occasionally

☐ Rarely

☐ Never

7. Do you have any backup system for your data/ information?

☐ Yes

☐ No

If yes, how often is the backup done?

☐ Daily

☐ Weekly

☐ Monthly

☐ Rarely

8. Are there any security measures and guidelines concerning ICT in general e.g.

ICT policy, ICT Security policy or so?

☐ Yes

☐ No

9. In your own view what do you think can be done to ensure efficiency in securing

ICT/IT facilities and services i.e. both equipment and services information/data?

☐ Yes

☐ No

If yes, is it readily available and understood by everyone?

☐

Yes

☐

No

APPENDIX B: Interview guide:

For ICT department staff members

1. Are there any measures in place to ensure ICT services and facilities are secure
e.g. policy document, rules and guidelines etc?
2. Which areas in ICT do you think its/their security is important?
3. What are some of the main security threats that you face as a department?
4. How do you counter these threats?
5. How do you ensure security of these services and facilities within the departments
and faculties?
6. In your own opinion what do you think can be done to improve on ICT security?
Give suggestions

Appendix C: Observation Checklist

1. Is there any access control measure when entering sensitive offices / rooms?
2. Which method is used to backup data?
3. How possible is it to access the servers/work directly from the servers?
4. Are there UPS machines on computer systems?
5. What is the frequency of systems breaking down?