An Investigation into Information Security Practices implemented by Research and Educational Network of Uganda (RENU) Member Institutions

Submitted in partial fulfilment
of the requirements of the degree of

Master of Science (Computer Science)

of Rhodes University

Alex Kisakye

Grahamstown, South Africa
October 2012

Abstract

Educational institutions are known to be at the heart of complex computing systems in any region in which they exist, especially in Africa. The existence of high end computing power, often connected to the Internet and to research network grids, makes educational institutions soft targets for attackers. Attackers of such networks are normally either looking to exploit the large computing resources available for use in secondary attacks or to steal Intellectual Property (IP) from the research networks to which the institutions belong. Universities also store a lot of information about their current students and staff population as well as alumni ranging from personal to financial information. Unauthorized access to such information violates statutory requirement of the law and could grossly tarnish the institutions name not to mention cost the institution a lot of money during post-incident activities.

The purpose of this study was to investigate the information security practices that have been put in place by Research and Education Network of Uganda (RENU) member institutions to safe guard institutional data and systems from both internal and external security threats.

The study was conducted on six member institutions in three phases, between the months of May and July 2011 in Uganda. Phase One involved the use of a customised quantitative questionnaire tool. The tool - originally developed by information security governance task-force of EDUCAUSE - was customised for use in Uganda. Phase Two involved the use of a qualitative interview guide in a sessions between the investigator and respondents.

Results show that institutions rely heavily on Information and Communication Technology (ICT) systems and services and that all institutions had already acquired more than three information systems and had acquired and implemented some of the cutting edge equipment and systems in their data centres. Further results show that institutions have established ICT departments although staff have not been trained in information security. All institutions interviewed have ICT policies although only a few have carried out policy sensitization and awareness campaigns for their staff and students.

Acknowledgements

First and foremost, I would like to thank God for giving me life and health throughout this whole year. Secondly I would like to thank Uganda Christian University for allowing me time to come down to South Africa and for the scholarship to study at one of the most prestigious university, Rhodes University.

I would like to thank my classmates from whom I have gained invaluable experience throughout this year, I wish you all success in your final thesis.

I would also like to thank my supervisor, Dr. Barry Irwin, for all the guidance you have accorded me this year and for having faith in my doing this all in one year.

Finally to my dear wife, Kadongokamu, for the love and allowing me time away from home. God bless you.

Glossary

ARPANET – Advanced Research Projects Agency Network

BBUC – Bishop Barham University College

CISA – Certified Information Systems Auditor

CISO – Chief Information Security Officer

CISSP – Certified Information Systems Security Professional

DDoS – Distributed Denial-of-Service

DoS – Denial of Service

HTTPS – Hypertext Transfer Protocol Secure

ICT – Information and Communication Technology

IHSU – International Health Sciences University

IP – Intellectual Property

ISP – Internet Service Provider

IT – Information Technology

LAN – Local Area Network

MUBS – Makerere University Business School

MUK – Makerere University Kampala

MUST – Mbarara University of Science and Technology

NREN – National Research and Education Network

PGP – Pretty Good Privacy

REN – Research and Education Network

RENU – Research and Education Network of Uganda

SQL – Structured Query Language

SSL – Secure Sockets Layer

UCU – Uganda Christian University

VLAN – Virtual Local Area Networks

WEP – Wireless Encryption Protocol

WPA – Wi-Fi Protected Access

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The use of computer systems has greatly increased over the years since the first computer was invented. Their uses in both homes and industry has varied from commercial computational use to complex nuclear systems and industrial control. The cost and portability of computer hardware has greatly reduced such that currently almost every household and business in the developed world can afford to own a Personal Computer (PC). The volume data that is stored on computers has also enormously increased and this is attributed to the evolving and reduction in costs of storage medium. It is increasingly cheaper to store digital information on computers than in a traditional paper file system. It is not only cheaper to store data digitally but also easier to retrieve and disseminate over the Internet to a wider population.

The number of new nodes that connect to the Internet has been seen to increase substantially over the years. The latest technology entrant, cloud computing and devices built to access cloud services, have even further made a traditional paper file system even more redundant.

Educational institutions are known to be the heart of complex computing systems in any region they exist, especially in Africa. The existence of high end computing power, often connected to the Internet and to research network grids, make educational institutions soft targets for attackers. Attackers of such networks are normally either looking to exploit the large computing resources available for use in secondary attacks or to steal Intellectual Property (IP) from the research networks. Universities also store a lot of information about their current student and staff population, as well as the alumni. Unauthorized access to such information violates statutory requirement of the law and may cost the institution a lot of money in remediation and law suits as well as ongoing reputation

damage. Carefully designed and implemented information security practises can be used to identify and mitigate some, if not all, of the information security attacks that are targeted towards educational institutions.

1.1 Problem Statement

Universities store an increasing volume of sensitive information about current research interests, their staff and student population. This information includes academic records, financial records, medical records, employment history and correspondence pertaining to the operation of the institution.

Originally such records were kept in paper based file systems under the strict care of the institution's top administrator. With the advent of computer systems, many paper based systems have been turned into electronic systems. Information like this should be protected by a series of practices such that it are only made available to those parties that have the permission to access it.

Over the last two years, Uganda accessed high speed broadband Internet connectivity by undersea cable. This exposed many insecure systems to the hostile Internet environment and, as a result, a number of websites have come under attack by different hacking groups all over the world. Some sites that have come under attack include government websites and university websites. In all attacks the intention of the attacker remains unclear nor what information has been lost or exposed to unprivileged individuals through such attacks.

This study will investigate the information security practices, put in place by the member institutions of Research and Education Network of Uganda (RENU) to safe guard this information, as well as other computing resources on campus from both internal and external security threats.

1.2 Objectives of Research

The primary objective of this study was to investigate the information security practices that have been put in place by RENU member institutions to safe guard institutional data and systems from both internal and external security threats. The secondary objective of

the study will be to assess the security readiness of these institutions to avert any security related incidences.

1.3 Research Questions

To achieve the objectives of this research, the following questions were used as a guide;

1. What is the institution's reliance on ICT systems and services?
2. What IT Security infrastructure has been deployed at the institution?
3. What is the staff composition of the ICT department?
4. What policies has the institution implemented to guide students and staff on the proper use of ICT resources?
5. How does the respondent assess the institution's readiness to fight information security challenges?

1.4 Relevance and Background

Information security is defined as protection of information assets, aiming to maintain confidentiality, integrity, availability and accountability of the assets [Ahlfeldt and Söderström, 2007]. Information security incidents in the case of a university can be in the form of information theft, data tampering, viruses, worms and data loss [Burd, Cherkin, and Concannon, 2005]. The source of security incidents can be external, such as hackers, or internal, originating from both staff and students [Eminağaoğlu, Uçar, and Eren, 2009]. Universities are known to be soft targets for a number of reasons, such as the existence of large number of computing resources that can be used in a secondary attack as zombies [Cooke, Jahanian, and McPherson, 2005, U.S. Department Of Justice, 2010], and also the existence of a large number of network users. As a result enforcement of security policies is often difficult to achieve. Universities also get access to Intellectual Property (IP) belonging to individuals and companies during research processes and this can potentially be targeted by competition as university environments are normally less secure than a company's research and development laboratories. The Information Technology

department of any university should be adequately equipped and prepared to avert such incidences.

Universities in Uganda have, over time, automated various aspects of their business processes through information systems. These systems store various records, including staff and student personal information that should only be available to privileged users. It is thus important that the universities take the necessary measures to make sure this information is secure and protected from unauthorized access. External attack sources in Uganda have increased dramatically in the last two years with the landing of SEACOM Internet cable at the East African coast [BBC News, 2009]. This development brought down Internet connectivity costs allowing all universities that either had no or slow Internet connectivity afford high speed broadband connections to the Internet. By doing this, university computer systems have been exposed to the Internet and only good security practices can safeguard these systems from attacks.

In a study carried out in the United States of America in 2006, out of the 182 universities and colleges that participated in the survey, 58 percent had experienced a security incident in the previous year and of these 33 percent had reported a data loss or theft [Piassa, 2006]. It was also noted that 9 percent of the data lost was students' personal information.

In October 2010, the University of Ohio announced that there had been unauthorized access to one of their servers [Ohio University Press, 2010]. The University announced that the information accessed included records of both staff and students. Information included both past and present records. It was later said the university would spend 4 million dollars to offer credit protection to it's users [Pyle, 2010].

On June 7th 2011, the website of Makerere University in Uganda was hacked. The hackers, who claimed to be from Syria, replaced the home page with a banner in what seemed to be a SQL injection attack. Since there are no statutory requirements in Uganda for public entities to make such breaches public, the University did not make any public comment about the attack but replaced the web page on the same day [Alai, 2011].

In August 2011, Purdue University announced that one of their servers had been hacked in April 5, 2010. The breach was discovered three days after it had occurred. Preliminary investigations revealed that the attacker had intended to use the server in a secondary attack. However after forensic investigations which lasted 6 months, it was discovered that Social Security Numbers (SSN) belonging to 7,093 former students might have been accessed. All the numbers accessed belonged to alumni classes that had taken mathematics at the university between the years 2000 and 2005 [Data Breaches, 2011b].

In August 2011, data that was stored on North Carolina State University computer server that contained private information for about 1,800 school children from Richmond and Wilson counties in the United States was accidentally put online. The data was gathered from 2003-2006 as part of a research study on classroom practices. The data contained names, Social Security Numbers and dates of birth. The breach was discovered after one of the parents of these students found it online and immediately called the university. The server's Internet connection was severed and Google was contacted to make sure no archived information could be obtained through Google Cache [Data Breaches, 2011a].

1.5 Overview of the Study

The study was conducted in three phases between the months of May and July 2011 in Uganda. Phase One included the use of a questionnaire which was sent to respondents in the participating universities. Phase Two involved the use of interview sessions between the investigator and respondents. At this phase a tape recorder was used to capture the proceedings of the interview. Phase Three was the data analysis stage in which data collected was analysed for meaningful patterns.

1.6 Limitations and Assumptions

The study was conducted on RENU member institutions only. There are currently more than twenty universities in Uganda. Only nine universities were RENU members as of 1st May 2011. RENU defines a member as an institution that has fully satisfied the requirements for membership which include:

- Must be offering university level education and/or conducting university level research.
- Organisations that are Universities must be established by Act of Parliament or chartered by the National Council for Higher Education.
- Must have an ICT Policy and Master Plan.
- Must have a functioning Local Area Network connected to the Internet.
- Must have an established information resource management function.

- Must meet the cost of membership as agreed by the launch meeting or reviewed by the signatories to the Memorandum of Understanding (MoU).

All nine members were invited to participate in the study. Only six members agreed to participate in the study.

1.7 Document Layout

The rest of this document is organised into four chapters as follows;

- Chapter Two introduces the concept of National Research and Education Networks (NRENs) and gives a history of information security and explains how educational institutions are soft targets for information security attacks.
- Chapter Three presents the methodology that was used during the study and discusses the choice of research methodology.
- Chapter Four presents the results obtained during the course of the study and offers interpretation of these results in relation to the overall information security readiness of the institutions.
- Chapter Five reviews the study and results obtained and offers conclusions based on these results. It also offers suggestions for possible future studies in the area of information security in educational institutions.

Chapter 2

Review of Literature

This chapter reviews the literature on information security in relation to universities. The chapter starts by defining National Research and Education Networks (NREN) is and goes on to introduce the Research and Education Network of Uganda (RENU) whose member institutions are is used as a case study for this research. It will also detail the efforts of some universities to implement safe information security practices and will also highlight the successes and challenges that have been met.

2.1 National Research and Education Networks

A National Research and Educational Network (NREN) is an entity that is responsible, on a national basis, for the provision of data communications networks and services to the research and education community of it's country. The NREN network typically connects other networks at regional or metropolitan level [Twinomugisha, 2007].

The history of NRENs dates back to the early 1970s [John, 2008] where smaller sub-networks of researchers operated in isolation and were idealfor supporting local research needs. In the late 1970s, as computer systems were advancing further, the need for researchers to work together, especially on common research areas that transcend the geographical boundaries of countries and continents, was beginning to take form. As much as there was an effort to interlink institutional research networks, due to the prevailing technology the only means of interlinking these systems was in the hands of commercial entities – telecommunication companies – through the use of telephone lines. The cost of transmitting data over telephone infrastructure was prohibitively high which was a

major hindrance to collaborative research efforts that were growing. In some parts of Europe, governments had started to realise the benefits of collaborative research efforts under NRENs and responded by offering high speed subsidized communication media and funding the activities of NRENs. By mid 1980s Europe alone had eight research education networks increasing to fifteen by 1990 [John, 2008].

In earlier times, it was believed that the advent of commercial Internet Service Providers (ISPs) would replace the educational networks but that was not possibledue to the difference in business models of these entities. NRENs serve educational and research entities and require huge investments and funding to get high speed connectivity links. Some carry out cutting edge research projects [John, 2008] that may not have a specific time frame to fetch returns or sometimes do no succeed as had been planned. ISPs, on the other hand, tend to provide Internet services to everyone and tend to use stable network applications in serving their clients. NRENs and ISPs tend to share a close relationship in that the research projects that come out of NRENs will normally influence the type of applications and services ISPs offer their clients. By 1990 there existed at least one NREN in each of the countries in Europe that was either fully funded by the government or at least actively supported by its government. The early research work at NRENs was based on particle physics and space research, however, as the collaboration brought closer educational and research entities, other disciplines realised the opportunity and potential of the networks and hence began using them for their work.

2.1.1 Source of Funding for NRENs

Since NRENs are known to conduct educational and research activities and since governments of any country are known to support such activities, it is desirable that the government fully takes up the funding role of the NREN. Also it is easier for government to channel its contribution to the education and research work carried out in the country to an NREN which normally encompasses all institutions, both public and private [Twinomugisha, 2007]. However the experiences differ from NREN to NREN, for example in BdREN [Khan, 2008] the NREN of Bangladesh, the funding model used is that of cost sharing between the government and participating institutions. The government funds some of the work of the NREN while the clients of NREN, the research institutions pay an annual subscription. In Internet2 [Internet2, 2008], the NREN in USA, funding is obtained from University Corporation for Advanced Internet Development (UCAID) which is the organisation that brings together close to 170 universities in the USA as well

as UCAID's corporate partners [Internet2, 2008]. The NREN does not get funded directly by the government although special funds such as grants may be awarded to the REN through competition with other research groups. Also some NRENs start off as entities within small interest groups of educators and researchers with participating institutions funding the work of the REN in form of annual subscription or through winning competitive research grants and overtime get funding from the government while in others government offers the seed funding of the NRENs' initial activities.

2.1.2 Membership

The membership of NRENs are researchers, students and teachers who normally are represented by their institutions in the NREN. These institutions are from both the private and public sector. The membership of NRENs differs from NREN to NREN with some of the NRENs only including public institutions while others having a mix membership between public and private research entities. The mix relationship is favourable as it is more inclusive and easier for an NREN to be considered a National REN. NRENs in some countries like USA [Vietsch, 2003, John, 2008] have expanded to include other entities such as libraries, museums and government offices. NRENs especially in Africa [Twinomugisha, 2007] have been discouraged from starting off as exclusively government institutions as the success of any NREN is greatly a result of how many members make up the REN.

2.1.3 Types of Services

The type of services that are offered to members of the REN differ from NREN to NREN and are sometimes seen as competitive services that would be offered by a typical ISP. The services are normally driven by the needs of the REN community and are implemented as the need arises [Schelkens, 2006, Twinomugisha, 2007]. Some services that a typical NREN would offer have been summarised in Table 2.1.

Service Category	Examples
Network and connectivity services	Client connectivity to the NREN, bandwidth management, DNS services, VPN services, NTP services, IPv6 services and Network support services.
Security services	Anti-Virus control, CSIRT, Intrusion Prevention, Vulnerability testing and netflow monitoring tool.
Authentication and "Mobility" services	Identity management services, server certificate service, Inter-(W)LAN/network access: EDUROAM service.
Infrastructure hosting	Web hosting, mail relay, disaster recovery, storage area networks, academic software distribution and ftp services.
Network communication tools and conferencing	Video/audio conferencing tools/application, Instant Messaging, Mailing list services and E-Mail gateway services.
User interaction - knowledge dissemination	Workshops, seminars, Support and User Portals, User conferences, NREN publications, newsletters and magazines.

Table 2.1: Typical NREN services to Members. Source: [Twinomugisha, 2007]

NRENs operate within the geographical boundaries of a country. However NRENs within a region or a continent form an alliance or consortium. The alliance provides further collaboration opportunities between not only its members but also between its members and members of other alliances. For example the NRENs in Eastern and Souther Africa are all under the UbuntuNET Alliance [Zimani, 2007] and these could be able to cooperate on research with Internet2, the consortium of NRENs in the USA.

2.2 The African NREN efforts

National Research and Education Networks (NREN) are fairly a new concept on the African continent. The oldest NREN on the continent, Kenya Education Network (KENET) was established in 1999 [Zimani, 2007]. The efforts to start NRENs in Africa have mainly

been fuelled with the need to find affordable means to connect to the Internet with many NRENs starting off as bandwidth consortia. As a result, many NRENs are still offering connectivity as the major service to their members and are not yet offering more advanced services such as those seen in NRENs found in Europe and America. The landing of the various Internet sea cables along the African coast to connect Africa to other continents using faster Internet links has also worked as a catalyst to the establishment and growth of NRENs on the African continent. Figure 2.1 shows the various sea cables that have already landed on the African continent as of October 2011.

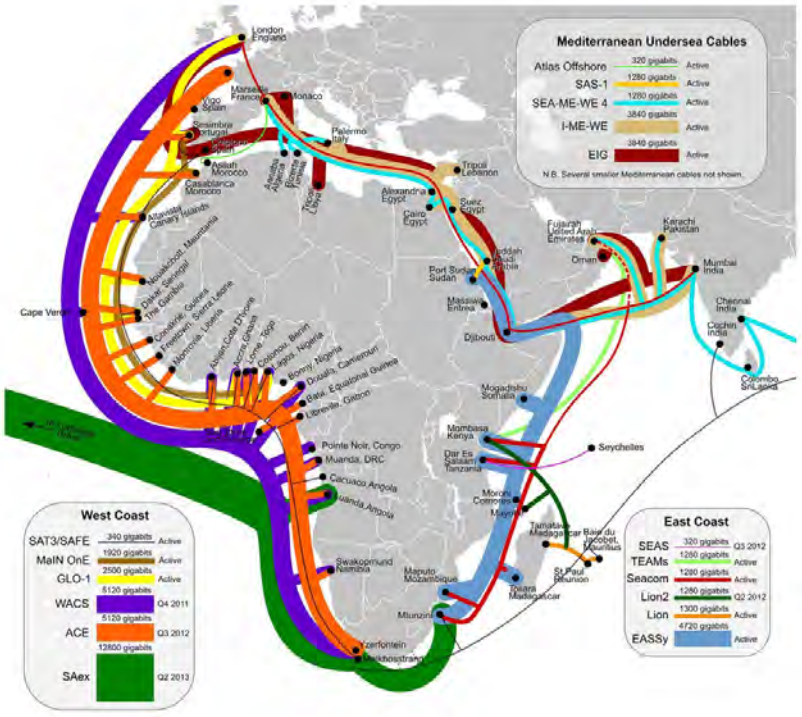

Figure 2.1: Map of Africa showing different Submarine cables connecting Africa to Asia, America and Europe. Source: Steve [2011]

Africa has 53 countries divided into five regions; South, Central, East, North and West Africa. A number of NRENs exist on the continent already and they are grouped into consortia.

West and Central African Research and Education Network (WACREN) is the consortium that takes up all the NRENs in West and Central Africa. The current membership includes 11 members from the following countries; Ghana, Senegal, Nigeria, Benin, Burkina Faso, Cameroon, Cote d'Ivoire, Gabon, Mali, Niger and Togo [Omo, 2010].

European and Mediterranean connection (EUMEDCONNECT) is the consortium that is responsible for NRENs in the counties in Northern Africa. The network was created to connect NRENs in the Mediterranean region with those in Europe so as to increase academic collaboration between the regions. Current members include; Algeria, Egypt, Morocco and Tunisia [David, 2005].

UbuntuNET Alliance on the other hand is responsible for Countries in East and Southern Africa. The NREN in focus in this study, Research and Education Network of Uganda (RENU), belongs to UbuntuNET. UbuntuNET was created in 2005 by the then already established NRENs of Kenya, Malawi, Mozambique, Rwanda and South Africa. It was later incorporated in 2006 as a non-profit association of NRENs with a purpose of serving all established NRENs of Africa. The current membership of UbuntuNET Alliance includes thirteen members; Democratic Republic of Congo (DRC), Ethiopia, Kenya, Malawi, Mozambique, Namibia, Rwanda, Somalia, South Africa, Sudan, Tanzania, Uganda, Zambia [Zimani, 2007]. Information about UbuntuNET NRENs and the countries they represent has been summarised in Table 2.2.

Country	**NREN**	**Established**
Ethiopia	EthERNet	2001
Kenya	KENET	1999
Malawi	MAREN	2005
Mozambique	MoRENet	2006
Democratic Republic of Congo (DRC)	Eb@le	2006
Namibia	X-net	2003
Rwanda	RwEdNet	2008
Somalia	SomaliREN	2006
South Africa	TENET	2003
Sudan	SUIN	2004
Tanzania	TERNET	2007
Uganda	RENU	2006
Zambia	ZAMREN	2005

Table 2.2: UbuntuNET Members. Source: [Zimani, 2007]

2.3 Research and Education Network of Uganda (RENU)

Research and Education Network of Uganda (RENU) was founded on the 14th January 2006 by a team of Vice Chancellors of universities and heads of institutions that are carrying out research in Uganda [Ali, 2010]. At this meeting, a Memorandum of Understanding [RENU, 2006] was drawn up and signed by all the Vice chancellors and heads of research institutions to establish a formal and legal entity recognised by the government of Uganda as the national REN by the end of that year. In 2007 RENU was registered and recognised by government and allowed to carry out activities of an NREN in the country [RENU, 2011].

2.3.1 The Objectives of RENU

The objectives of RENU as drawn up in the memorandum of understanding [RENU, 2006] are:

- To promote and facilitate research and education networking among Ugandan universities and research organisations;
- To create stronger negotiating positions and get better terms for participating organisations in dealing with:
  - Government and regulators on issues related to policy and regulation vis a vis research and educational organisations;
  - Suppliers of hardware, software, online resources, and bandwidth, including getting benefits arising out of economies of scale;
  - Development partners on issues of common benefit;
  - Inter-connecting with other research and education networks worldwide.
- To explore ways of overcoming the high cost of information systems through pooling resources and sharing, where feasible, costs for common software, and promoting collaboration in areas that may include but are not limited to:
  - E-learning systems to help deliver common online courses;
  - Library information systems that allow members to easily digitize and share their collections.

- To explore new avenues for other value-added services as may from time to time be needed in support of higher education and research networking in Uganda.

2.3.2 Sources of Funding

The funding model of RENU is member-subscription-based as the major source of income and competing for grants and awards for capacity development in terms of equipment sourcing and training [RENU, 2006]. Currently government support has come in terms of waiving of taxes on equipment purchased to run the REN's network while other donations have come from external funders. Some of the key donors and funders [Ali, 2010] that have funded RENU's activities since its formation include Internet Educational Equal Access Foundation (IEEAF), Global Medical Research Exchange (GMRE), United States Agency for International Development (USAID), IDRC, UbuntuNet Alliance, Fostering RENs in Africa (FRENIA), Swedish Program for ICT in Developing Regions (SPIDER), West Indian Ocean Cable Company (WIOCC).

2.3.3 Membership of RENU

Currently, the RENU Memorandum of Understanding (MoU) between institutions [RENU, 2006] does not discriminate against public or private funded institutions joining membership of RENU but sets aside minimum conditions that have to be satisfied for an institution to be admitted.
Under the memorandum, an entity applying to be a member of RENU shall only be accepted provided they satisfy the following minimum conditions:

- They must be legally operating in Uganda as an Educational entity
- They must be offering university level education and or conducting university level research
- They organisations that are universities must be established by Act of parliament or chartered by the National Council of Higher Education
- They must have an ICT policy and master plan
- They must have a functioning LAN connected to the Internet

- They must have an established information resource management function
- They must meet the cost of membership as agreed by the council

The current membership of RENU, as obtained from the RENU website [RENU, 2011], includes eleven members. These include nine universities and two research based organisations.

Institution	**Funding**	**Type**
Uganda Christian University	Private	University
Kyambogo University	Public	University
Makerere University	Public	University
Makerere University Business School	Public	University
Gulu University	Public	University
Uganda Martyrs University	Private	University
Joint Clinical Research Center	Public	Research Entity
National Agricultural Research Organisation	Public	Research Entity
International Health Sciences University	Private	University
Bishop Barham University College	Private	University
Mbarara University of Science and Technology	Public	University

Table 2.3: Summary RENU member Institutions. Source: [RENU, 2011]

2.3.4 Member Services and Benefits

The main benefits enjoyed by RENU member institutions include [Ali, 2010, RENU, 2006]:

- Lower tariffs offered by ICT network providers for both Internet bandwidth and Leased-Lines by the formation of bandwidth consortia.
- Technical support from RENU secretariat technical team which includes but not limited to device configuration such as servers, routers, firewalls, and LANs for access to the global Internet and also the ultimate education network that RENU is setting up.
- Capacity building of member institution technical teams through specialized training sessions and sharing of best practices.

The Bandwidth Consortia

Bandwidth has been seen as a major obstacle for many educational institutions to fully utilising the resources that the Internet provides. In order to overcome this obstacle, members of an NREN pool their individual connectivity resources into "bandwidth consortia". The bandwidth consortium is one of the key major services that RENU is offering its members.

Prior to 2009, Uganda was accessing the Internet through satellite communication, which is known for being very expensive. At the time, bandwidth in Uganda was priced at an average of USD3000 for 1Mbps. Few education institutions were able to afford bandwidth for Internet connectivity and many choosing to go for email dial-up solutions that were offered by ISPs. RENU saw the opportunity in pooling resources from the REN's members so that bandwidth could be purchased in bulk and thereafter apportioned to the members based on contributions made.

The landing of the SEACOM cable on the East African coast [BBC News, 2009] and its extension into the inter-land to reach Uganda, not only brought the Internet closer to the markets and end-users in Uganda but also managed to greatly reduce the costs of connectivity. The cost of bandwidth reduced to USD680 for 1Mbps for the ordinary consumer of Internet services. RENU through its partners and donors managed to negotiate further with Uganda Telecom, one of the national providers of communication services in the country and the back bone infrastructure provider of RENU to provide bandwidth to its members at USD610 for 1Mbps [RENU, 2011].

RENU also received a donation on SEACOM of 10Gbps of capacity to NREN networks in Europe funded by IEEAF. Universities have been encouraged to maintain their previous expenditures on bandwidth at levels prior to the landing of the submarrine cables in order that they can obtain more bandwidth from subsequent price cuts in the future.

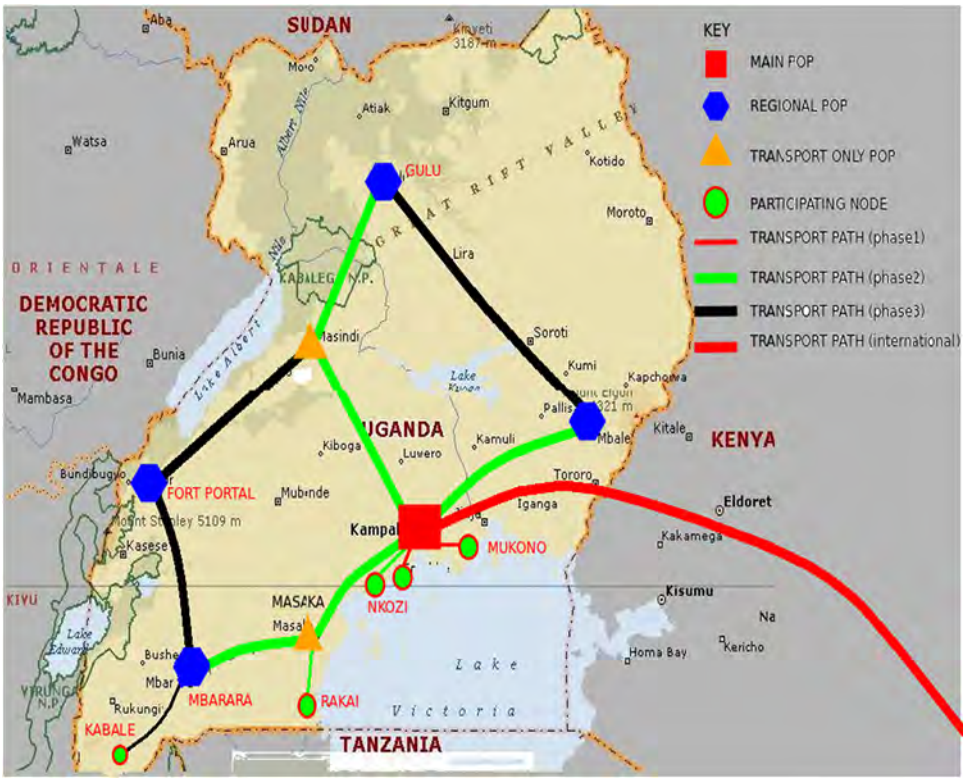

Figure 2.2: Network Diagram for the RENU Network. Source: [RENU, 2011]

2.3.5 Achievements of RENU Since Inception

Some of the achievements and RENU to date include [Ali, 2010];

- RENU hosted the UbuntuNet-Connect in 2009. This a forum that connects all the NRENs in Eastern and Southern African. It happens every year and at these events different NRENs share their experiences in running different activities of an NREN.
- RENU was registered as a legal entity in Uganda and officially recognised as the formal NREN for Uganda.
- RENU managed to secure an Autonomous System Number (ASN) and public IP space for its members use from AfriNIC.
- The network has eleven member institutions.
- RENU has already participated in a collaborative research with KENET the Kenyan NREN .
- RENU has organised capacity building training events for it members.

2.4 A look at the history of Information Security

This section documents the information security trends since the 1970s and how the attack vectors and attackers' motivations have evolved. This will give the reader a clear picture on how these incidents have evolved over the years. The time line has been grouped into decades starting with the 1970s.

2.4.1 1970s

The 1970s were dominated by the use of the mainframe. These systems, because of their bulkiness, were confined to huge rooms that were physically secured [Morris and Thompson, 1979]. They were originally manned by a single individual computer operator whose duty was to execute punch cards on behalf of the users and giving the users the results of their programs [Campbell and Aspray, 1999].

Later, terminals were able to be connected to the mainframe so that users could run their own programs and receive results immediately [Campbell and Aspray, 1999]. The security that was implemented on these systems was two-fold [Gollmann, 2011]; prevention of unauthorized access to the system and keeping the information that was already kept on the systems away from users who were not meant to see it. In the former instance, the use of password protection was efficient enough as this meant that all who had access to the system would have been given valid credentials to use while using terminal access. In the latter instance, the use of encryption was ventured into to make sure that classified information and files were encrypted to prevent unauthorized access [Gollmann, 2011]. For encryption the Data Encryption Standard DES which has been published by the NSA was preferred [Morris and Thompson, 1979].

2.4.2 1980s

In this period, computer manufacturers had developed the PC. This was a standalone computer able to do all it's processing on its own. It was also smaller compared to the mainframe and cheaper in cost. These developments managed to increase the penetration of the computer into research entities, universities, businesses and homes that could not afford the mainframe [Gollmann, 2011].

This period is seen as the biggest backward slip of computer security because of the following; the computers had become standalone which meant that one computer belonged to a single individual, since the individual was not sharing it, they did not see the need to secure the information stored on it, secondly the operating system that had dominated the PC of the 80's, Microsoft Disk Operating System (MS-DOS) did not support multi-user environments and this was laxity in the security of the operating system. Unfortunately most of the security challenges that were later seen in the 90's had been due to this culture that the PC had started in the 80's [Gollmann, 2011].

In this period, the first network virus that was reported and documented was the Morris worm in 1988. It rapidly propagated the ARPANET infecting at least 10 percent of the devices on the network at the time. It replicated too fast that the systems were unable to processes any other legitimate work. To contain it, systems administrators had to physically shut-down their hosts that were connected to the network [Hoar, 2005].

2.4.3 1990s

The start of this decade was marked by the making of the Internet public. This meant that all the smaller privileged hosts of the The Advanced Research Projects Agency Network ARPANET had been exposed to a greater network that spanned the whole globe. The use of applications like email and web sky-rocketed with a number of businesses using the Internet as a medium to market their products and to get in touch with their clients thus eliminating the middleman [Gollmann, 2011].

Because the Internet was still being looked at as a communication tool or medium the security that was implemented was the kind that was implemented in other communication networks like the telephone networks. This included making the communication medium secure and prevention of eavesdropping on messages along its paths [Gollmann, 2011]. This was an oversight on the engineer's part because while the telephone network has its main processing taking place at the core of the network with dumb terminals at the end, the Internet had its processing taking place at the end terminals and thus having a dumb core. The biggest security threat was taking place at the end terminals not along the communication paths. The PC user had suddenly lost control of who would send information to their computers and how they would do it. The original controls of user access to computers was now lost because unauthorized users could access a computer over the wire without ever coming into contact with it. Also a new challenge of malformed

messages come to light with the first hackers being able to over flow memory and cause the system to act in ways it was not intended to do.

It was also in this decade that the information security property of availability was tested more as many systems suffered from Denial of Service (DoS) attacks [Gollmann, 2011]. Many businesses especially the smaller ones who had ventured into online business to reduce costs of production now faced a challenge of being kept offline with DoS attacks that were rampant. A new cost of doing business, security incidences was slowly emerging. It is in this decade that the use of firewalls and intrusion detection systems started to appear at the edge of most networks.

It is important to note that the hacker in this decade attacked a computer or network as his primary objective. And while most of the computer breaches were done by computer experts wanting to show off their skill and occasionally for financial gain, it was never their intention to maintain access for long periods of time [Gollmann, 2011].

2.4.4 2000s

This is the period that is seen as one where the use of resources on the Internet by consumers is massive. It also marks a time when the Internet became an essential part of doing business for the commercial entities. The Internet started moving from a parallel communication tool to old communication services like the telephone to completely replacing these services as the only communication tool in some economies in what has been termed convergent technologies [Bertassi, Gabos, Korolkovas, Maia, Martucci, and Spina, 2005].

The technology behind the Internet had not changed since the early 1990s but the applications that depended on the Internet were seen to increase and improve a lot during this time period [Gollmann, 2011]. Because of the security trends, a new IT career with security-related duties started to emerge and was being demanded by businesses and enterprises. A number of software and hardware was developed to protect the networks and system users against attackers and malware. A number of online databases containing exploitable systems and exploit code also sprung up in this decade to make sure the security administrators and users alike are kept abreast with security developments that were around them. As the network administrators got smart, and the network edge defence devices like intrusion detection systems became more accurate at detection, attackers found a new weakness, exploiting end-user desktop applications.

The hackers of this decade also attacked systems as part of a long term strategy that starts with the hacker gaining control of many computers and later controlling them to attack a secondary target. In such a case, the attacking machine is referred to as a zombie primarily because it is just following directions of the botnet master and it is part of a botnet [Cooke et al., 2005]. If the aim was not to use these machines as zombies, the attacker would maintain access to the victim computer and collect sensitive information from the computer like credit card numbers as the user is browsing the Internet.

2.5 Universities and Information Security

Universities and higher learning education institutions all over the world have continuously moved away from the traditional file system to more automated computerised information systems. The systems used in various universities have been given various identifying names and acronyms but the core functionality of these systems remain, Academics Records Management information systems, Health Information management systems, Alumni Information management systems, Finance information management systems and many others. The implementation of all or some of the systems varies between the needs of the university and the costs of implementation of a given system.

Information security has been known to be inadequate on university campuses and this has been blamed on mainly the lack of information security awareness for both students and staff [George, North, and North, 2006].

In a study on IT Security Governance, Strategy, and Practice in Higher Education John et al. [2003], the authors suggest a number of reasons why universities are unable to keep up with the information security best practises that are recommended for industry. Some of the mentioned challenges are discussed in the following section;

2.5.1 Decentralisation *vs.* Centralisation

Many institutions operate in a decentralised mode of operation, the schools and colleges within the university are given autonomy of operating their own IT systems. Some schools and colleges get donation and grants from donors and government which they choose to manage separate of the central ICT infrastructure John et al. [2003]. In this case the proper management of such decentralised systems is not very easy. It is not possible for

the security administrator to easily know which systems are at risk. This can also be partly blamed on the fact that some institutions do not have organised ICT departments and data centres to work as central distribution points for ICT resources. The enterprise is different in this regard with one central data centre to manage the needs of the entire enterprise. Even in cases where the enterprise spans different geographic areas, there will be efforts to manage the ICT resources centrally.

2.5.2 Standard Equipment *vs.* Diverse Equipment

The type of equipment on a university network differs in type and make. For example one school many be using Linux operating system on their computers because of a particular software while the other computers are running windows operating system or macintosh. Even if the university tries to make the operating systems or machine vendor uniform it is still impossible to have homogeneity since the students computers and other Internet ready devices such as mobile phones will be different. This kind of heterogeneity makes it hard for the security administrator to enforce policies across the board John et al. [2003]. In the enterprise on the other hand, there is a uniformity in the operating system and the machine architecture that is being used, even when a particular department is using specialised software it will be easy to manage since it is controlled by policy.

2.5.3 Human Resource Budget to Employ Security Persons

Many universities are usually constrained when it comes to finances and hence will tend to cut costs in other areas not considered priority. Because of this, many ICT departments are not able to employ a single dedicated individual to manage security on the university campus. The end result is either the security function being merged with that of the network administrator or the system administrator or the function will be completely eliminated from the functions of the ICT department. The enterprise because of the need to either pass industry compliance tests or to protect the share holders interests will normally employ a dedicated individual to manage the security function of the organisation.

2.5.4 Diversity of Business Activities

The university will typically engage in many activities related to academics and research, such activities become difficult to identify for a security administrator, for example if a university is engaged in pharmaceutical research a mail server with a spam filter that sorts mail for Viagra spam messages and other products can easily eliminate legitimate mail [John et al., 2003]. The corporate organisations tend to be in one line of business and in which case the security administrators will always be aware of what business interests the organisation is involved in thus making the deployment of security technologies easy.

2.5.5 Diversity of Users

The typical users of a university are not easy to categorise, universities employ staff academic or administrative either on full time or part time, they have students on full time and those on part time. Universities also allow guests academic or otherwise to use university resources. Some universities tend to extend access to government services by allowing the use of library resources to people who are not active students or staff of the university. Because of this diverse nature of users, it becomes difficult for a security administrator to secure and isolate users efficiently, the enterprise on the other hand will normally have access for only staff, in few cases where guest access is granted it would be with a locked down access John et al. [2003].

Despite the challenges that Universities and Higher Institutions of Learning face in implementation of information security best practises, the cost of an attack or misuse of computing resources resulting to failure or data loss need to be considered by all institutions. It should be noted that the cost of insecure systems is many times driven by legislation and legal measures that a country has put in place.

During the course of this study it was evident enough that it was easy to find the case studies of security breaches and the costs involved of Universities in the United States of America (USA) while it was not possible to easily find the same information of universities in Uganda.

The USA has a number of standards put in place to control how information and data is handled, for example the Family Educational Rights and Privacy Act (FERPA) [Federo Register, 2011] which is most applicable to educational institutions mandates the institution to protect the staff and students information when it is stored. In cases where the

institution needs to share this information, the owner for example a student (or parent if student is under 18 years) must give consent. If also the students information is accessed unlawfully the institution has to notify the student immediately in writing.

Uganda on the other hand has recently passed a Computer Misuse bill [Parliament Of Uganda, 2008] which protects systems from unauthorized users but does not protect the privacy of users who are the owners of this information. The absence of such legislation could be the reason information security breaches that have occurred in Ugandan universities have not been documented.

2.6 Case studies: Attacks and Institutional Cost

For information security to be taken serious in institutions and business alike, management and key decision makers need to understand the cost that attacks impact on their institutions. Often, key decision makers will not prioritise the security of information and systems of the institution until they understand the cost for non-compliance in monetary terms. In this section we look at some of the attacks that have occurred in institutions and businesses and their financial impact on the affected entities.

2.6.1 Missouri State University

Missouri State University staff unknowingly exposed 6,030 records of students including their personal details and Social Security Number to the public. The lists of students had been generated for internal use and was to be shared among the staff securely. Unfortunately one of the staff mistakenly posted the lists on a unsecured public server and they were consequently indexed by Google hence making them visible and available to anyone on the Internet. The exact date that this happened is not known but suspected to be between October and November of 2010. Also the University was to carry out investigation so that the staff responsible could face disciplinary action.

The University learned of the breach in February 2011, almost three months after the actual incident had occurred. The University worked with Google to remove the lists from Google cache and indexing. This university offered to pay the costs of Consumer identity theft protection insurance for all the students affected. The negotiated cost was USD 7 per affected students which comes to a total of USD 42,210. The University also

had to incur costs of informing all affected students of the breach of privacy [Missouri State University Press, 2011].

2.6.2 Massachusetts General Hospital

In February 2011, the General Hospital Corporation and Massachusetts General Physicians Organization Inc. agreed to pay the U.S. government USD 1,000,000 to settle potential violations of the United States of America Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

The announcement was made by the U.S. Department of Health and Human Services (HHS) after an investigation into the loss of protected health information (PHI) of 192 patients of the hospital's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. Office for Civil Rights (OCR) opened its investigation of the hospital after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that the hospital failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from the hospital's premises and impermissible disclosure of PHI potentially violating provisions of the HIPAA Privacy Rule. The documents which were lost on March 9th 2009, by the hospitals employee who had taken them off hospital premises to continue work at home, were left on the subway train as the employee came to work and were never recovered. Their contents included, a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients [HHS Press Office, 2011].

This case is relevant because most educational institutions operate on campus health facilities in which they store student health information. Improper handling of such records can easily expose such records to unprivileged individuals.

2.6.3 University of California

In July 2011, the University of California, Los Angeles (UCLA) paid USD 865,500 to the Office of Civil Rights (OCR) and agreed to a Corrective Action Plan to settle allegations that UCLA Health System (UCLAHS) employees repeatedly snooped in the electronic health records of celebrity patients. The OCR's investigation was prompted

by two separate complaints on behalf of celebrity victims. The investigation revealed that from 2005-2008 employees repeatedly and without authorization accessed electronic health records of these patients. Settlement announcements did not identify either of the specific complaints, but in the past, UCLAHS has identified violations involving the records of Drew Barrymore, Arnold Schwarzenegger, Tom Hanks, Leonardo DiCaprio, Farrah Fawcett and others.

This was not the first time such an incident had happened within the same institution. In June of 2010, a UCLA surgeon was sentenced to four months in jail for repeated, unauthorized access to the records of his supervisor and celebrity patients.

UCLAHS's corrective action plan requires UCLAHS to implement policies and procedures approved by OCR, to conduct "regular and robust" employee training, to sanction offending employees, and to designate an independent monitor who will assess compliance with the plan over 3 years [Cynthia, 2011]. Like the previous case, this is relevant because most educational institutions operate on campus health facilities in which they store staff and student health information. In the absence of employee awareness training and lack of legislation, employees may be tempted to access client records without the proper authorization to do so which in effect leads to exposure of such records to unprivileged individuals and in some cases loss of trust between the institution and its clients. The cases studies discussed in this section are summarised in Table 2.4.

Institution	**Attack**	**Detection**	**Cost(USD)**
Missouri State University	Insider breach	3 months	42,210
Massachusetts General Hospital	Physical Loss	1 month	1,000,000
University of California	Insider threat	2 years	865,500

Table 2.4: Summary of Security Breaches and Costs.

2.7 Common Attack Vectors

Attack vectors are the sources that attackers use to get into computer systems and networks or a means of delivering an attack [Spohn, 2011]. In most cases a security officer will have to guard a system or network from multiple attack vectors in order to make it immune to security attacks. Attack vectors can be grouped into; external network, internal network, wireless, social engineering and application [Secunia, 2010].

2.7.1 External Network Attack Vectors

These are attack vectors that originate from outside the organisations network. They normally attack organisational services that are exposed to the Internet or will find a way of punching a hole in the boarder firewall in order to access services that are hidden behind the firewall. Some services that are normally victim to such attacks include DNS, Mail services, and Web services. The attack vectors that are likely to be used against these services can include Denial of Service and or Distributed Denial of Service, application exploitation due to Zero-day [Fox, 2009] vulnerabilities that have been discovered in web applications.

2.7.2 Internal Network Attack Vectors

These are attack vectors that originate from within the boundaries of the organisations network. They are normally very difficult to avert since the users on the internal network are normally considered non hostile and thus are allowed access to restricted services and resources. These kind of attacks normally seen on the internal side leverage on the minimal privileges that the users are given and will exploit system vulnerabilities to escalate normal user accounts to super user accounts. Another angle to this is that the success of these attacks greatly relies on the susceptibility of the human element. Without proper policy in place, an employee can easily walk off the organisations premises with important or classified documents [Archibald et al., 2008, Fox, 2009].

2.7.3 Wireless Network Attack Vectors

These attack vectors originate from the external network users. Since wireless networks are bound to overlap the campus area that the organisation is covering, these attacks are lethal to the network. Attackers can sit just across the road from the campus and still access the network entirely. In many network set-ups, the defences are all put on the external facing connection between the ISP and the organisation and the wireless access points are forgotten. With a successful attack on wireless the attacker would access the entire network as if they were sited inside an office in the campus. The most normally used form of encryption WPA and WEP have both been exploited [Allen and Wilson, 2002, Beck and Tews, 2009] in the past, however they continue to be the most favourite defences used by network managers.

2.7.4 Social Engineering Attack Vectors

Social engineering is one of the most successful vectors used to target information systems. It is normally used as a build up to secondary attacks targeted at the victim organisation [Pavkovic and Perkov, 2011].This is because the defences for this kind of attack are more difficult to implement. Social engineering attacks involve mainly the attacker using deceptive strategies to get the user to assist him in carrying out an attack [Hasan and Prajapati, 2009]. The user might or might not be aware that they are helping the attacker in the process. An example of a social engineering attack would be an attacker who posses like he is from IT maintenance and asks the users for their passwords in order to troubleshoot their computer problems. The user will willingly give the password because they have been deceived into thinking this is a genuine staff from IT department. Defences against such attacks normally require well structured and implemented user awareness programmes which many institutions or enterprises do not have the man power to carry out.

2.7.5 Attack Summary

In summary, it is important for a security officer to clearly understand the attack vectors if they are to be able to protect systems and networks from attack effectively. In a study carried out by the Secunia group on security incidents of 2010 [Secunia, 2010], it was found that external attack vectors had been the most used by attackers for the year 2010. They covered 81 percent of all attack vectors used that year.

2.8 Security: The Case of Ugandan Universities

Uganda, located in East Africa is made up of 111 districts. These districts are distributed according to the regions that they geographically fall, namely; Central Region, Western Region, Eastern Region, Northern Region and Southern Region. The country currently has more than 30 both public and private universities distributed across all the regions [UNESCO, 2009]. Universities in Uganda share many of the challenges that other universities in the world face in terms of security, but in addition also face unique challenges that have made their systems more prone to attacks. We discuss some of those challenges and draw a case why this study will be beneficial to the universities in Uganda.

2.8.1 Landing of Sea Cables

Prior to 2009, Uganda's access to the Internet was through expensive satellite links. Few universities that could afford to pay up the cost to access Internet could only afford slow speeds. The major Internet application that was in use was email. When SEACOM cable landed at Mombasa, Kenya [BBC News, 2009] and eventually extended to reach Uganda, the Internet costs greatly dropped thus allowing the entire country access broadband Internet and at affordable costs. Many institutions were finally able to afford access to the Internet at faster speeds which greatly enhanced the quality of education.

Fast Internet access does not only enhance access to Internet but also to academic research networks worldwide. Institutions that did not have access to the Internet or had limited access normally confined to academic and administrative offices were able to extend this access to their entire staff and student populations. This kind of unpredicted access to the Internet exposed computers in laboratories and offices that had never connected to the Internet,to a hostile world wide network that has attackers constantly looking for unpatched and vulnerable systems to attack. This kind of access to the Internet has increased the external attack surface for the institutions.

2.8.2 Rapid growth in ICT Use

The landing of the SEACOM cable did not only make the Internet cheaper but had an impact on the usage of ICT generally in Uganda. The reduction in the cost of bandwidth increased the number of ISPs and consumer targeted data packages that were greatly subsidised in price. In a way this increased the number of services that users demand from the Internet and eventually the number of Internet connected devices that are used. Devices like laptops and Internet enabled phones are now being demanded more.

In university environments, number of students with Internet enabled devices surged more times than the administrators of ICT can plan for. This rapid surge in the number of Internet ready devices that students own only makes it hard for a security officer to effectively manage the devices on the network. Even if an administrator tries to effectively control the security of devices on the network, controls cannot be effective since the students not only access the University network but also access other networks while off campus that do not necessarily conform to the same security policies as the university network hence students are able to pick up a virus infection off wireless networks at a café© or home and will bring it onto the university network the next time they connect. Students who

only use their laptops to access Internet on university campus risk bringing vulnerable unpatched laptops to the network especially after long university holiday breaks.

2.8.3 Relatively Young ICT Departments

ICT in most Universities in Uganda has not yet been appreciated as an enabling requirement for the wholesome education of students. Most institutions look at ICT and Internet especially for the commercial traffic that it carries. The aspect of research and using Internet to access research networks has not fully been appreciated.

As a result most universities are channelling their resources into infrastructural development and are not developing the ICT departments capacity to be able to serve the needs of the institution. For institutions like this, security is not a priority because of the unnecessary immediate costs. It can be argued that the cost of insecurity has not been assessed either as a means of showing universities the benefits of running secure computer systems. Also in some cases where the ICT department has been established, there is still an authority issue as many small departments opt to run their own systems because they were obtained as a special donation or grant. This results in having critical systems distributed all over the university campus thus increasing the sources of attack.

2.8.4 Absence of Legislation

The absence of the right legislation and security compliance standards like a Privacy Act to protect students and staff data that is stored on University computers makes universities ignore implementing security controls for the systems that they run.

Such efforts if enforced by government would encourage universities to maintain secure systems for fear of being penalised or sued by their student and staff population for an unauthorised access to their data. However even without legislation, universities should be able to provide assurance to its population for the records that they obtain from them lest they risk establishing a distrust relationship with staff and students.

2.9 Related Studies

The researcher was not able to find similar work done within Uganda and this can be attributed to the fact that ICT security in Uganda is generally a field still in its infancy.

However, in other parts of the world, a number of studies have been done focusing on educational institutions and businesses as well. The following section discusses some of these studies.

In a study carried out on two Universities in Tennessee [Nyabando, 2008], the results indicated that the faculty and staff of the target institutions were aware of information security issues and safe practices. The results also showed that the members who had used computers for more than 20 years were more aware of the safe practice than those that had used computer for lesser years. Password management and policy awareness were identified as some of the challenges for the participants.

In another study carried out on "*The state of information security in South-Western Nigerian Educational institutions*" [Ajayi et al., 2004], the results showed that 86 percent of the respondents experienced security breaches on academic data or information, which signified a major security problem for academia. 40 percent of the institutions had their computers connected to the Internet thus making them easy targets especially for external attacks. 82 percent of the institutions had no ICT Security policy in place for their institutions and 83 percent had no security awareness programme which meant that staff and students were not aware of the security challenges that using computers and the Internet pose to their data.

In a study "*Higher Education IT Security Report Card*"carried out in the United States of America by CDW-Government [Piassa, 2006], the results showed that 58 percent had experienced at least one security incident in the previous year and 33 percent had reported a data loss or theft. The report also indicated that the biggest challenge to Security in Educational Institutions was, Administrations not regarding IT security with the same urgency as other ICT requirements and this was evident with how little was in the budgets to cater for ICT Security related expenditure.

In a study carried out by Gartner research in 2006, it was found that security threats to institutions of higher education are increasing, but the resources that are available to deal with these threats are often highly constrained [Lowendahl, Harris, and Zastrocky, 2006]. The following are the key findings from the study;

- Best practices for justifying and allocating security resources can result in significantly greater effectiveness and efficiency in combating security threats in a sustainable manner.
- The most important step that an institution can take to strengthen its security efforts is the appointment of a Chief Information Security Officer (CISO).

- The failure to designate a CISO with a strong mandate could lead to serious difficulties in driving the institution's security efforts.
- Malicious-code and denial-of-service attacks are an increasing threat for many institutions, although computer theft appears to be in decline.
- Calculations of lost value because of security incidents are not performed by most institutions, and the failure to do this can cause problems in justifying and allocating resources.

2.10 Summary

This chapter has reviewed the literature on information security with relation to Universities. The chapter also explained in detail what an NREN is and introduced the Research and Education Network of Uganda. A section was devoted to reviewing information Security success stories and challenges that are faced by educational institutions worldwide.

In order to understand the practices implemented by Research and Education Network of Uganda member institutions, a suitable methodology was developed for use. The next chapter discusses the research methodology used in collecting data in detail.

Chapter 3

Methodology

The primary objective of this study is to investigate the information security practices that have been put in place by RENU member institutions to safe guard institutional data and systems from both internal and external security threats. The study was conducted by the researcher in person in Uganda from May to July 2011.

This chapter discusses the methods that were used to collect the data used in the study and the rationale behind the specific questions that were asked of the respondents who participated in the study. The chapter is divided into three sections; section one discusses the research design used while section two introduces the participants who participated in the study. The last section explains the grading system used and the rational of the grading system.

3.1 Research Design

The study was carried out in two phases using a mixed method research; the first phase involved the use of a questionnaire while the second phase involved the use of interview question guide used in sessions between respondents and the investigator. At this stage a recorder was used to record the responses of the respondent. Both instruments gained the approval of the ethics committee at Rhodes University.

3.1.1 Phase One

In this phase of the study questionnaires were sent out to the key individuals that had been identified by the head of department of ICT in the participating institutions. Respondents were required to answer the questions on the questionnaire that had specifically been designed to ask the question "What are the security practices that are in practice at this institution?" The questionnaire included five sections around which the Institutions security readiness was to be assessed.

The questionnaire was designed with the help of the Information Security Governance (ISG) Assessment Tool for Higher Education [EDUCAUSE, 2005]. The ISG Assessment Tool for Higher Education was developed by the Security Risk Assessment Working Group of the EDUCAUSE/Internet2 [Internet2, 2008] Computer and Network Security Task Force.

This tool is designed to support the Information Security Governance (ISG) framework recommended by the Corporate Governance Task Force [Entrust, 2008] and was modified for use with Institutions of Higher Education based in the United States of America. The Corporate Governance Task Force is one of the Task Forces formed by the National Cyber Security Partnership (NCSP) in the US [NCP Website, 2003]. The NCSP is led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet and the U.S. Chamber of Commerce in voluntary partnership with academicians, CEOs, federal government agencies and industry experts [NCP Website, 2003, Shore et al., 2004]. The role of the Task Force is to create a private sector framework for organisations to improve ISG on a voluntary basis. The Corporate Governance Task Force is comprised of forty-five members from industry, educational and not-for-profit organisations in the US [Entrust, 2008].

The original tool includes the following sections; Organizational Reliance on IT, Risk Management, People, Processes and Technology and was meant to assess the entire institution with the head of the institution such as Vice Chancellor being the main respondent. For purposes of this study, this tool was customised for use on RENU member institutions as well as assess the ICT Departments and their operation as opposed to the entire institution.

The targeted key respondent was the ICT Director or any member of the ICT team as nominated by the director. The sections in the customised questionnaire are, Institutional profiling, Infrastructure, Human Resource and Awareness, Policy, and Self-assessment.

These sections have been discussed in detail in the section that follows. A copy of the questionnaire has been included in Appendix C.

3.1.2 Questionnaire

Institutional Profiling

This section was meant to try to understand more the dependency of the institution on ICT services and systems. It is in this section that the investigator hopes to understand which systems the institution relies on for its day to day business, as well as the number of system users both staff and student. Another part of this section sought to find out the number of computing resources that are available to staff and students.

It also investigated the connectivity means that students and staff use to access resources such as wired, wireless or off-campus dial-in. Results from this section will help the researcher understand the number of computing resources as well as the degree of dependency that the institution has on ICT systems and services.
It is from this that we shall be able to understand the level of destruction a security incident can cause the institution.

Infrastructure

This section investigates what security hardware and related software that the institution has already put in use. It seeks to find out if the institution has realized the importance of securing its resources and what resources have been already protected. This section also investigates if the institution realizes that the information security practices go beyond the basic defences employed commonly by network administrators such as installing a gateway firewall and installation of anti-virus on computer terminals and servers.

Human Resources and Awareness

This section investigates if the institution has realized the need to centralize resources in one place as opposed to having small departmental resources that are distributed over the campus. It also investigates if the institution has an organized ICT department and team whose duty is to look after the resources that are available to them. We also investigate

if the positions available in this department have security function either integrated or independent of other positions in the department. We also investigated if the security function has taken the initiative to raise security awareness among its users.

Policy

This section investigates if the institution has acceptable use policy and IT security policy and whether they have been published or not. It also seeks to find out if policies have been disseminated to the population and that they are clear and easy to understand. We also investigated if there were measures to check for non-compliance and the consequences thereafter.

Self-Assessment

The self assessment section was added to try and find out if the key respondent has an idea of the relatively common terms that are used in the security arena. After the self assessment, the respondent was asked to grade his/her institution's information security readiness. The respondent was also asked if they can suggest ways of improving their preparedness.

3.1.3 Phase Two

In this phase of the study, an interview guide was designed to be used. The intention of the guide was to obtained more qualitative information on some of the questions that were posed on the questionnaire. The guide was sent to the respondent in advance of the interview sessions so that the respondent could get a good grasp of the questions that were to be asked. All the interviews took place at the participating institutions premises. A tape recorder was used to capture the interview session so that the interviewer could be able to fully engage the respondent without having to transcribe as well. The interview guide can be found in Appendix B

3.2 Participant Samples

The participants of this survey are RENU member institutions. Since this was a study of RENU member institutions, permission was sought first from the Chief Executive

Officer (CEO) of RENU to carry out the study on its members. After the necessary permission had been obtained from RENU, member institutions were also contacted for their permission to be included in the study and seeking their full participation in the study. All the nine universities that are members of RENU as at 1st May 2011 were contacted seeking their permission for inclusion into this study. The request to participate was sent on email to the heads of department of ICT departments of the institutions using contact information obtained from RENU, the email requested that they nominate someone from within their department who was knowledgeable about the departments security practices and policies and who could willingly participate in the study. Six member institutions responded positively while two members opted not to participate in the study and one member did not reply to the invitation email.

The institutions that responded were Uganda Christian University, Makerere University, Makerere University Business School, International Health Sciences University, Bishop Bharam University College, Mbarara University of Science and Technology.

3.3 Participant Data

The study was carried out in Uganda on RENU member institutions. Six member institutions voluntarily agreed to participate in the study out of the nine members that were contacted. The following is brief information about the participants.

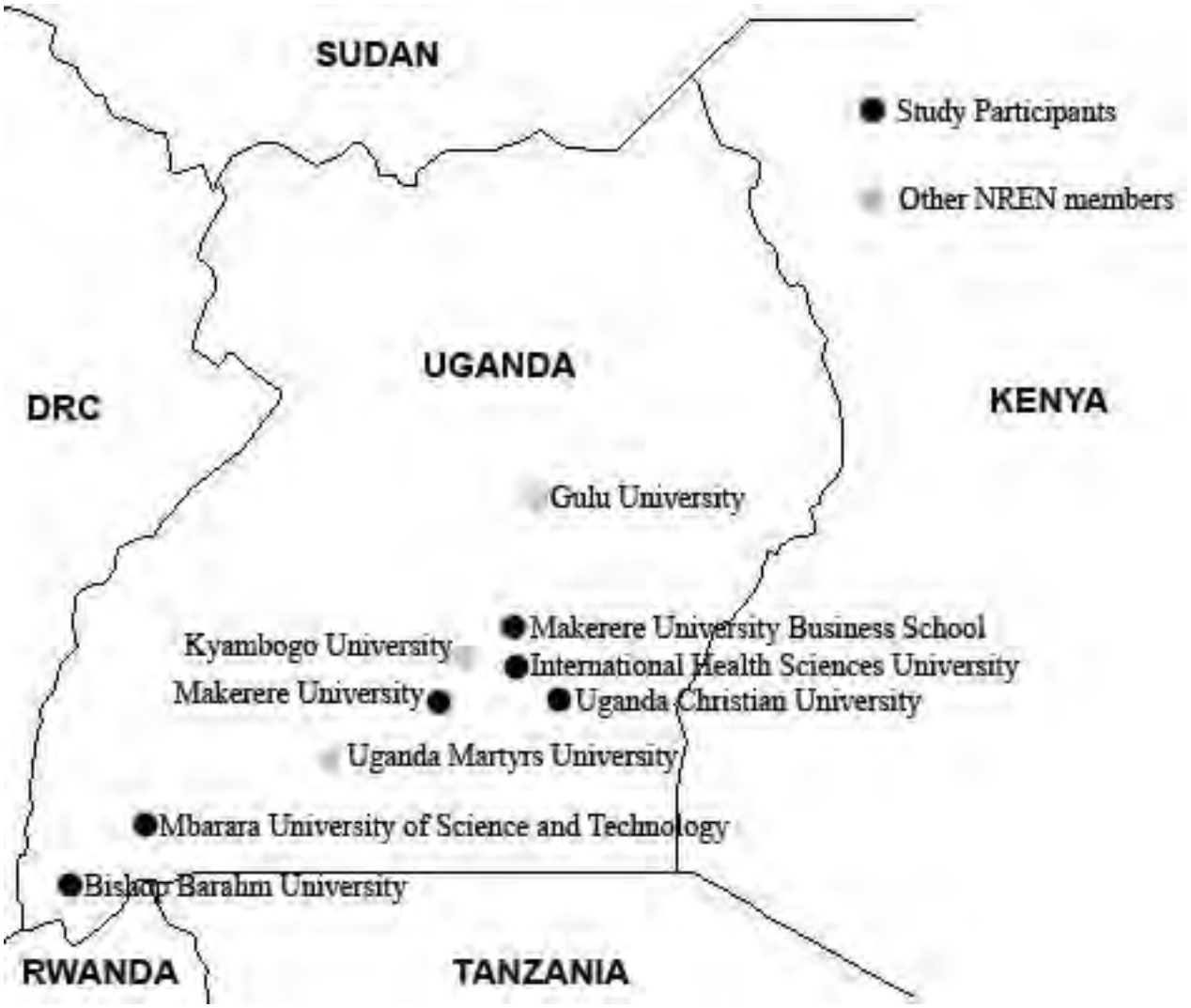

Figure 3.1: Map of Uganda showing geographic location of participants. Source: [RENU, 2011]

3.3.1 Uganda Christian University (UCU)

Uganda Christian University is located 23 kilometres from Kampala, in Mukono town, on the the main road to Jinja. It is a private university, chartered and fully accredited by the President of the Republic of Uganda, through the Ministry of Higher Education and Sports, and the National Council for Higher Education. UCU is owned by the Province of the Church of Uganda, and has campuses in Eastern, Western and Northern Uganda. The University was born out of Bishop Tucker Theological College. The college was founded in 1913 in response to a growing need for pastors in the Church. Uganda Christian University has all the necessities for an excellent education. It is recognised internationally and

nationally. The Most Rev. Henry Luke Orombi, Archbishop of the Church of Uganda is Chancellor, and the Rt. Rev. Dr George Carey is the Patron. Source: [UCU, 2011]

3.3.2 Makerere University (MUK)

Makerere University is Uganda's premier public institution of higher learning. It is located on Makerere hill, one of the many hills on which Kampala, the capital city of Uganda is built. The main campus is about 5km to the north of the city centre covering an area of 300 acres (Approximately two square kilometres). With almost all facilities serving beyond the capacity they were designed for, the 83-year old university is the biggest and most sought after institution of higher learning in Uganda. The University has made tremendous strides towards the integration of ICT into its functions and operations over the last five years. Makerere University offers not only day but also evening and external study programmes to a student body of both Ugandan and foreign nationalities. It is also a very active centre for research. Source: [MUK, 2011]

3.3.3 Makerere University Business School (MUBS)

Makerere University Business School was established by Makerere University (Establishment of Constituent College) order 1997 as a constituent college of Makerere University (MUK). The School was created from a merger between the Faculty of Commerce (FoC) and the National College of Business Studies (NCBS). The merger involved the physical movement of the faculty of commerce from the Makerere Campus to Nakawa where the NCBS was located. The actual merger and movement took place in January 1998.

In the year 2000, the law was amended to give financial and administrative autonomy by the Makerere University (Establishment of constituent college). As a result of this amendment, the school structure changed tremendously. The law created a council with authority similar to that of Makerere University Council. In the year 2001, the structure of the school again changed with the enactment of the University and other tertiary institutions Act, which made the school transform from a constituent college of Makerere to a public tertiary institution affiliated to Makerere University [MUBS, 2011].

3.3.4 International Health Sciences University (IHSU)

International Health Sciences University was established and admitted the first class of students in August 2008. The University, owned by The International Medical Group has its main campus at 4686 St. Barnabas Road, Namuwongo, a south-eastern section of Kampala, Uganda's capital and largest city. IHSU's campus is located on the top floor of the building that houses International Hospital Kampala. The road distance from the central business district of the city to Namuwongo is approximately 6 kilometres. The university offers it courses both on site and via e-learning platform Moodle [IHSU, 2011].

3.3.5 Bishop Bharam University College (BBUC)

Bishop Bahram University was originally founded in 1924 by Dr. S. Smith and L. Sharp, who had come to Uganda with the Rwanda Mission. The purpose was to train Bible teachers and lay readers for the Western region of Uganda.

BBUC sits in the cradle of the revival movement commonly known as the "East African Revival". Moreover, BBUC is right where the first educational centre in the Kigezi area (south-western Uganda) was established. In the 1980s, the College rose to become a Regional Theological College of the Church of Uganda for the south–western region. In 2000, the Church of Uganda Provincial Assembly granted the College the status of a Constituent College of Uganda Christian University for the western region of Uganda. This status was ratified by the National Council for Higher Education (NCHE) on 27th of March 2006. The University is administered by twelve Church of Uganda dioceses, namely Kigezi, North Kigezi, Kinkizi, Muhabura, Ankole, West Ankole, North Ankole, Rwenzori, South Rwenzori, East Rwenzori, Bunyoro-Kitara and Masindi-Kitara [BBUC, 2011].

3.3.6 Mbarara University of Science and Technology (MUST)

Mbarara University of Science and Technology is a public University located in the South-western part of Uganda, 300 km from Kampala city. It is made up of three faculties of Development Studies, Science, and Medicine. MUST was established in 1989 following a statute of the National Resistance Council, the then legislative body in Uganda. This was In response to government's realization that higher education was a critical asset for

nation building, at a time when Uganda's economy and social infrastructure had collapsed, due to civil wars in the 1970s and 1980s.

The university is recognized by National Council for Higher Education in Uganda. With acclaimed national and international recognition for best practices in outreach and community relations from Association of Commonwealth Universities, European Union , Civil Society of Uganda, produces the best development workers and health care professionals [MUST, 2011].

Name	**Region**	**District**	**Funding**	
Makerere University	Central	Kampala	Public	
Uganda Christian University	Central	Mukono	Private	
International Health Sciences University	Central	Kampala	Private	
Bishop Barahm University	South-Western	Kabale	Private	
Makerere University Business School	Central	Kampala	Public	
Mbarara University of Science and Technology	Western	Mbarara	Public	

Source: [RENU, 2011]

Table 3.1: Summary: Participants Information

3.3.7 Participant Blinding

During the study, the participants were promised anonymity for both their identities and those of their institutions. For this reason the respondents names and their institutions will be masked from the response data. Codes U, V, W, X, Y, Z have been allocated to the participants and will be used in the rest of the study to identify the surveyed institutions.

Code	**Role of the Respondent in ICT Department**
U	Ag. Manager MIS
V	Network Manager
W	Head of ICT Infrastructure
X	ICT Manager
Y	Librarian
Z	Head of Computing Department

Table 3.2: Table Showing Role of Respondents in Institutions

3.4 Grading System

The questionnaire used for this study included five sections. In each of the sections, various questions were asked and the grading codes used were A, B, C, D, E and F in order to avoid biasing the participant's responses. However, during analysis, each of these codes has been given a numeric number to signify its weight, the numeric numbers will be used later in the grading of the performance of each of the participating institutions.

Grade	**Value**
A	1
B	2
C	3
D	4
E	5
F	6

Table 3.3: Grading Used

3.5 Summary

This chapter reviewed the methods that were used to collect data during the study. It also included brief information about Uganda and profile information about the members that participated in the study and the respondents. Also the grading that was used in during the study has been explained. The instruments that were developed from this chapter were used to collect data from the participating institutions. The next chapter discusses in detail the results obtained during the data collection process.

Chapter 4

Results and Analysis

Nine RENU members were contacted to participate in this survey however only six members responded positively. Despite the explanation that the survey was not in anyway comparing members achievements, two of the members opted out because they felt it would compare their achievements against the other members. One member did not respond to the invitation. The study had a return rate of 67 percent. The chapter contains the results from the study as well as analysis and interpretation of the results. The results will also include a discussion section in which the researcher compares the results with other studies that have been done around the world in both business and educational environments.

4.1 Institutional Profiling

Institutional profiling was assessed using the categories of budgeting, staff and student population, available computing resources, available information systems and wireless systems and remote access. This section answers the research question of *"What is the institutions reliance on ICT systems and services?"*.

4.1.1 Staff and Student Populations

It was found that 1/2 of the institutions had between 401 – 800 staff, 1/3 had between 1 – 200 staff and 1/6 had staff over 3001. It was found that 1/2 of the institutions had more than 5001 students.

The number of staff and students tended to tally with the size of the institution and also the number of years it has existed. Institutions that have been in existence longer have more students than the newer ones. Also it was clear institutions with more students had slightly more staff which is reasonable. The number of staff and students has been summarized in table 4.1.

Code	Number of Staff	Number of Students
Makerere University Business School	401 - 800	5001 - 15000
Makerere University	¿3000	15001 - 40000
Uganda Christian University	401 - 800	5001 - 15000
International Health Sciences University	1 - 200	500 - 2000
Bishop Barham University College	1 - 200	500 - 2000
Mbarara University of Science and Technology	401 - 800	2001 - 5000

Table 4.1: Number of Staff and Students

4.1.2 Budgeting

It was found that 1/2 of the institutions that participated in the survey spent between UGX101 – 1Billion shillings (USD 36,000 – 350,000) on their entire ICT budget, 1/3 spend less than UGX 100Million (USD 36,000). When it came to expenditure on security related products and appliances, it was found that 1/2 of the institutions spend between 10 percent and 20 percent of their budget on security related expenses and the other 1/2 spend less than 4 percent of their budget on security.

It should be noted that the components of the budget differ from institution to institution. In some institutions the ICT departments payroll would have to be incorporated into the ICT budget whereas in others the ICT budget doesn't include payroll of ICT staff. Also some budgets include expenses of computer purchase and other equipment purchases while in other institutions these costs are considered capital and hence put in the institutions capital budget. It also important to understand that some ICT department rely on the ICT fees levied on students fees to run their budgets, in such cases the student population will greatly influence the size of the ICT budget.

The portion spent on security products also varies between institutions, the biggest challenge was the fact that all institutions did not have on-going security programs hence determining what percentage of the total budget is spent on security required critical scrutinizing of the institutions budget to identify security-related products. Also one of

the institutions mentioned that they do not spend on security products because they use free and open source security-related software entirely in the institution. For such an institution, expenditure on security was zero. In others, security software purchases like anti-virus are handled within the central budget of the university hence not reflecting on the departments ICT security code.

4.1.3 Computing Resources

Half of the institutions surveyed had between 301 and 800 computers connected to the Internet, 1/3 has less than 300, and 1/6 had more than 3001 computers connected to the Internet for student and staff use. Again here it was noted that institutions that have larger numbers of students and staff populations equally had larger numbers of computers for access to the Internet.

4.1.4 Information Systems

Reference is made to table 4.2 which shows the information systems and their distribution among the universities that use them.

	Institution					
Security Area	**U**	**V**	**W**	**X**	**Y**	**Z**
Academic Records Management IS	O	O	O			O
Financial Management IS	O	O	O	O	O	O
Student Management IS	O	O		O		
Library Information System	O	O	O	O		O
Learning Management System	O	O		O		O
Alumni Management System						O
Email System	O	O	O	O	O	O
Website System (CMS)	O	O	O	O	O	O

Table 4.2: Information Systems used in participant institutions

It was found that each of the institutions was using at least three information systems to facilitate informed decision making processes. 1/2 were using a Financial Management System, Email System and Website content management system. The next highly used

system was the Library Information System with 5/6 of the participants using it. The least used system was the Alumni management system with only 1/6 of the participants using it. This indicates that there is a high reliance on information systems and that there is a substantial amount of data that is stored on the institutions network.

2/3 of the institutions stated that system failure would be critical to the business processes of the institution internally while 1/3 stated that such a failure would be unacceptable.

2/3 of the institutions stated that system failure would be critical to the business processes between the institution and the external parties like business partners and 1/6 stated that such an occurrence is unacceptable. Another 1/6 stated that this would have no impact on business processes between it and the external parties.

5/6 indicated that loss of Internet connectivity would be critical to the proper functioning of business processes within the institution while 1/6 stated that this would partially impact its business process within the university.

On the impact of Internet loss between the institution and the external business world or partners, 1/2 stated that it would be critical while 1/3 stated that this would be unacceptable and 1/6 indicated that this would have no impact at all.

The fact that institutions noted that information systems failure or loss of Internet connectivity affects their ability to work internally and externally with partners shows the dependency of institutions on information systems and also indicates that institutions should take extra precaution to prevent such occurrences.

4.1.5 Third-party Service Providers

2/3 of the institutions use third-party service providers like software developers and network expansion specialists to do department work, 1/3 do not use external third-party contractors. 2/3 also use additional staff who are not on the institutions payroll to do department work, such as interns and other support staff. This signifies that external contractors and temporary employees do not go through rigorous security and credibility checks done by the human resources department. No matter how complex a scheme of background checks and security policies an institution has in place, ultimately the information security of an institution hinges on the integrity and honesty of those who are given access [Albertson, Briana, Dow, Kenneth, and Peter, 2003]. Many times the best way to get into an organisation without being noticed is by posing as an employee who will most likely go unnoticed because of their perceived right to access certain resources.

4.1.6 Wireless Access Systems

It was found that 5/6 of the institutions had a wireless system deployed on the campus for staff and student access and 1/6 had no wireless system deployed. Of those using wireless access systems 4/5 were using some form of encryption WEP or WPA while 1/5 were not using encryption at all. It was also found that 1/2 offer their students and staff means of accessing institutional systems off campus such as academic record systems and email systems.

The use of wireless systems is normally encouraged because of its advantages such as reducing the cost of infrastructure in terms of laying physical network and also providing students and staff easy means of accessing network resources. However, the use of wireless access can easily be abused by attackers to gain entry into secure systems using remote access especially when the systems are not monitored or protected [Ben, 2004]. While most institutions using wireless indicated that they use some form of encryption, 1/5 of institutions indicated that they are not using encryption at all. This poses a serious concern because an attacker can gain access to the network without any effort. Even though the encryptions in use WEP and WPA have their security draw backs [Allen and Wilson, 2002, Williams et al., 2008, Beck and Tews, 2009], they provide a base barrier between attackers and the wireless network.

4.1.7 Summary

A summary of the key findings relating to institutional profile are shown below.

- 50% of the institutions had between 401 – 800 staff
- 50% of the institutions had more than 5001 students
- 50% of the institutions spend between UGX101 – 1Billion shillings on ICT budget
- 50% of the institutions spend between 10 and 20 percent of their budget on security related expenses
- 50% were using a Financial Management System, Email System and Website content management system.
- 66% of the institutions consider system failure critical to the business processes of the institution internally

- 66% of the institutions consider system failure would be critical to the business processes between the institution and external parties
- 83% indicated that loss of Internet connectivity would be critical to the proper functioning of business processes within the institution
- 50% stated that Internet loss would be critical on the communication with external partners
- 66% of the institutions use third-party service providers like software developers
- 66% also use additional staff who are not on the institution's payroll to do department work
- 83% of the institutions had a wireless system deployed on the campus for staff and student access
- 50% offer their students and staff means of accessing institutional systems off campus such as academic record systems and email systems

The overall reliance on ICT systems and services for the institutions was found to be high. The total points that could have been obtained by any institution in this section was 40. From figure 4.1, it can be seen that most of the institutions scored more than average, 20, for this section hence reflecting the high reliance on ICT systems and services for the institutions.

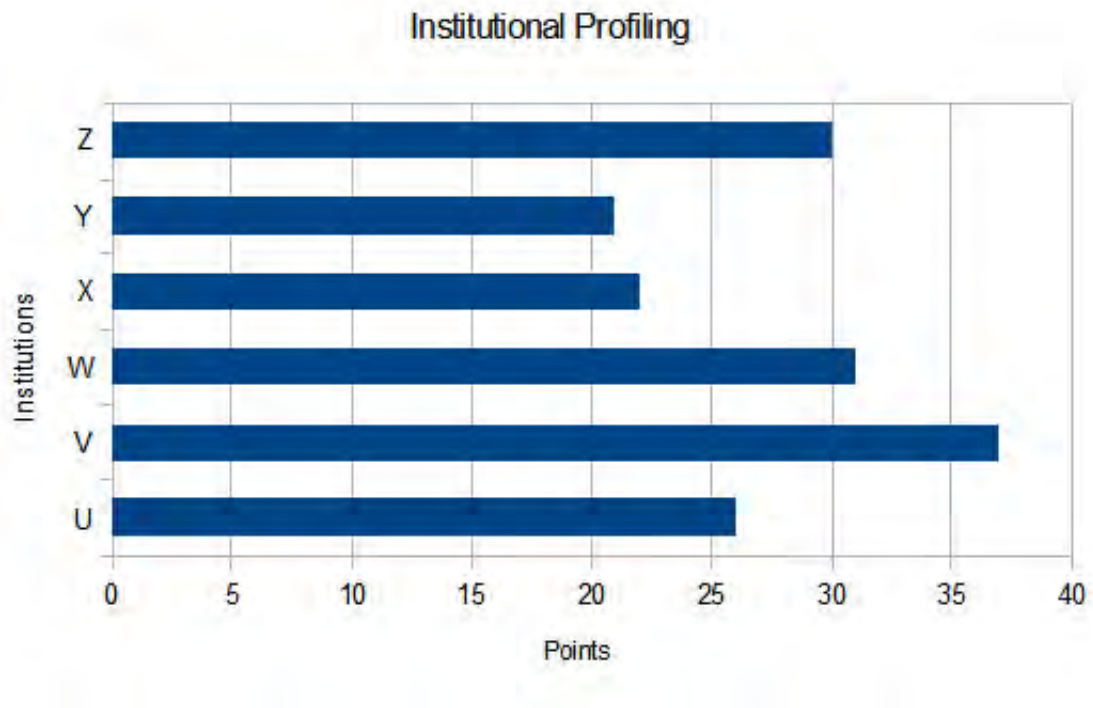

Figure 4.1: Institutional Profiling Summary

4.2 Infrastructure: Software and Hardware

Infrastructure was assessed using the categories of Network, Systems and disaster recovery. This section addresses the research question of *"What IT Security infrastructure has been deployed at the institution?"*

4.2.1 Network Infrastructure

On whether Internet-accessible servers are protected by one or more security layer(s), 1/3 indicated that they have "fully implemented" this while the rest of the participants are working towards having this implemented.

5/6 indicated that they have "fully implemented" specific measures to secure remote access to their servers while 1/6 indicated that they have "partially implemented" this.

5/6 indicated that they have "fully implemented" means to monitor and secure the servers that monitor their domain which include DNS and DHCP servers, 1/6 indicated that they have "partially implemented" this.

1/2 indicated that they have "fully implemented" policies that guide system and configuration changes done 1/6 have "not implemented" this.

The results show that the institutions have already implemented one or more security layer(s) to protect their systems. Security layers are ways of providing various security techniques to protect enterprise resources for example for network traffic that is coming into the LAN from the Internet the institution implements a firewall to filter this traffic to prevent unwanted traffic from entering the network, behind the firewall the security administrator can have and Intrusion Detection System/Intrusion Protection System IDS/IPS to alert of any successful intrusions through the firewall.

At application level, the security administrator can have an application firewall that is able to filter traffic sorting out malformed requests that are made to the application. For traffic that is generated within the institution, the security administrator can use authentication mechanisms to grant users access to the network and also use access control lists to limit their work to only duties that they are allowed to do. These layers of security however, are meant to provide extra security to systems and services but should not be thought of as the ultimate solution to security issues.

Vulnerability Management

Four of the respondants (2/3) indicated that they have "partially implemented" a strategy to scan their systems and applications periodically for vulnerabilities and as well as integrity of configuration files. While 1/6 indicated that they have "not implemented" this strategy. 1/6 also indicated that they continuously monitor in real time their networks and systems for unauthorized access and anomalies such as viruses and worms.

Vulnerabilities are weakness in software and hardware systems that are a result of bugs or misconfiguration and give attackers ways of violating rules of procedure for the systems in which they exist. Vulnerabilities that are detected can normally be mitigated by applying a vendor provided patch or change in configuration for poorly configured scripts. Also another challenge that presents itself is the existence of custom software applications that are supported by developers with no appreciation of secure coding practices. This presents institutions with vulnerabilities that may not be easily fixed and on time.

Typical tools used for identifying and classifying known vulnerabilities are vulnerability scanners. These tools look for vulnerabilities known and reported by the security community, and which typically are already fixed by relevant vendors with patches and

security updates. Also commercial software exists whose sole role is to constantly monitor applications for vulnerabilities and notify security administrators of a new vulnerability. The lapse between the discovered vulnerability and the vendors ability to patch against it present a zero-day vulnerability which is every administrator's nightmare. Regular scanning of applications is hence very necessary to be able to identify vulnerable software and systems so that the security administrator can consequently patch the systems and software.

Logging

Two institutions indicated that they have "fully implemented" logging for security-related activities such as hardware configuration changes, software configuration changes, access attempts and privilege assignments, 2/3 have "partially implemented" or "not implemented" this at all.

Logging is a very important aspect of systems and network security. Logs not only provide troubleshooting information to the system administrators but can also be used to audit user activities on the network such as privilege escalations and attempted logins. Log monitoring should hence be one of the duties of a security administrator and also carried out regularly. Logging can vary from logging configuration changes to logging authentication attempted and file access.
Normally policy will dictate the type of logs that are monitored from systems and how long such logs should be kept for analysis and reference purposes. Systems such as Linux offer automatic logging and log rotation facilities on default install.

Rogue Access Points

The majority (2/3) indicated that they have "not implemented" a means of preventing and detecting rogue access to their wireless networks while 1/6 indicated that they are "close to completion: or "fully implemented" this strategy.

Rogue access points are normally wireless access points that are installed on to a secure network environment without the permission of the network or security administrator. Rogue access points can be installed by innocent network users or attackers with the intent of gaining unauthorized access to the internal network. These access points extend network access to the interested parties with less means of being detected because of the

portability of access points and lack a clear policy on who should be installing devices on the network. Successful planting of an access point on a network allows the attacker to access the LAN remotely and use LAN resources like he/she is part of the network. Access can be intended for the primary network or in order to use the LAN to launch secondary attacks on another network over the Internet. By all measure, the security administrator should devise means of detecting such rouge access because of the security challenges that they present.

4.2.2 Systems Infrastructure

1/2 indicated that they have "fully implemented" the encryption of sensitive data and the encryption keys are kept safe while 1/3 indicated that they have "not implemented" this.

1/2 indicated that they have "fully implemented" a mechanisms to manage digital identities from through out their life cycle from creation to deletion while 1/3 have "partially implemented" and 1/6 have "not implemented" this at all.

Data encryption

Encryption is a way of converting data into a form (cipher text) that cannot be understood by listening parties other than the parties it is intended for. Encryption can take place during data transfer and or during storage. Data during transfer is normally encrypted with protocols such as SSL, HTTPS [Lee, Malkin, and Nahum, 2007]. The means of encrypting and decrypting data are as important as the keys that are used in the process. Keys are a means to encrypt and decrypt data and these keys should be stored well as mismanagement of the same renders the whole data encryption process useless. Data encryption presents a way to secure the owners of the data like students and staff from unintended disclosure which reveals personal information that is otherwise private.
There are two types of encryption asymmetric and symmetric [Fujisaki and Okamoto, 1999]. Asymmetric also sometimes refereed to a public key depends of use or two keys, public and private. A users public key is available to all those who intend to transmit a message to them over the Internet while the user will use his private key to decrypt this message, the hugest implementation for this is the PGP [Henry, 2000]. Symmetric encryption means that the same key that is used to encrypt data should be used to decrypt it. Information in an institution is mainly moving between accounting systems and banks,

between academic records systems or is stored on systems. Encrypting it along the way protects it from unintended disclosure.

Identity management

All but one (5/6) of the institutions indicated that their systems use automatic password changes while one indicated that this not implemented at all. Firther, of those that had some implementation, two indicated that they have "fully implemented" system session time out and user management practices while one had "not implemented" this at all.

Only two institutions indicated that they have "not implemented" the use of a single database for authentication across all systems while 1/6 have "fully implemented" this. Identity management is a very important aspect of managing users on a system or network. Identity management can be used to manage individuals identities as they go about their duties and how they interact with information resources. Users can further be organised in groups and assigned different permissions with access control lists in order to further facilitate the sharing of resources on the network. In an identity management system, identities go through a life cycle that includes creation, management and deletion at the end of life cycle of the identity. Academic institutions, because of the different activities and information systems that exist are encouraged to have some form of identity management to ease the way users are granted access and rights to use and view certain pieces of information. The large number of systems is met with a large number of users with a diversified range of requirements to operate computer resources.

A number of university systems have been hacked into because they have identities of past students that were never terminated or forgotten about. The best way to manage identities in a university is to use a central authentication and identity system such as Light weight Directory Access Protocol (LDAP) [Alvestrand, Hodges, Morgan, and Wahl, 2000]. LDAP offers a protocol to connect to and manage a global directory of users who are allowed to authenticate on systems. it can also be use to manage user profiles throughout their life cycle.

Central Anti Virus and Patching

5/6 indicated that they have "fully implemented" central anti-virus protection and control for both their servers and workstations. 1/6 indicated that they have "partially

implemented" this strategy. Of those that have fully implemented central anti-virus management, only 2/5 have "fully implemented" strategy to audit whether all clients and servers regularly get updated virus definitions.

1/2 indicated that they have "fully implemented" a strategy to update all server and client computers with the latest operating system patches.

For institutions that are running hundreds of computers, it becomes efficient to have some form of central management for anti-virus and patch management. This control should offer ways of auditing to make sure that the systems are updated and have patches. Central monitoring offers a number of advantages such as reducing overall systems management reducing the number of supervision visits that the systems administrator has to make around the institution to make sure that all systems are updated. This reduces the number of machines that can be overweighted to being up-to-date and yet they are not. It also reduces the number of machines that connect to the Internet to download updates with a central dissemination of patches and virus definitions. In order to completely protect the entire network, anti-virus protection should be extended to student and staff personal laptops and mobile computing devices. Devices especially students devices are used to connect to the Internet on various wireless connections that may not be as secure as the university network hence a student is bound to pick up a virus infection and infect the whole university network once they connect again at the institution.

4.2.3 Disaster Recovery

2/3 indicated that they are "close to completion" or have "fully implemented" a system backup strategy while 1/3 have "not implemented" a backup strategy. Of these 3/4 also indicated that their backup strategy covers all critical systems in the institution. Only 1/4 indicated that they periodically test the backup strategy to make sure recovery is possible.

Backup is a very important aspect of information security processes. This is because, in pursuit of automation, universities have acquired a number of systems to enhance the smooth running of the institution. These systems collect a vast amount of information that is used in making key business decisions. Loss of such information due to system failure, virus attack, software problems, external attacks, and internal employee attacks [Landry and Koger, 2006] can easily cripple the institution not to mention legal suits. The kind of data that is collected in any institution is sometimes not replaceable, this

include students information, staff information, financial information and other sorts of data stored. Good backup procedures can help restore data that has been lost due to any of the cause and reduce considerably to amount of down time.

All the institutions that participated in this survey had at least three information systems that are already implemented, such developments show that the dependency on computer systems is high on all institutions. The use of information systems brings to mind the need for adequately disaster recovery planning to reduce the risks that arise out of disaster situations.

A good backup system should include all systems that are used in the institution, in determining the systems to back up and those to ignore, the backup coordinator needs to make sure that the institution is able to work at 100 percent after the incidents and this means that all critical systems need to be backup.

It is important to make sure that the backup systems do actually work, it is considered useless to have a backup system that cannot be restored from. System restoration tests should be done as well as time to restoration accounted for, the business needs to know in times of disaster what time frame it will take to restore normal operations.

4.2.4 Summary

- more than 50% of the institutions have implemented one or more security layer(s)
- more than 66% of the institutions scan their systems for application vulnerabilities
- 16% have fully implemented a means to constantly monitor their networks
- 33% of the institutions currently monitor logging for security-related changes such as hardware changes
- 66% have not implemented a way to prevent and detect rogue access to their wireless networks
- 83% have implemented specific measures to secure remote access to their servers
- 50% have polices that guide system and configuration changes
- 50% of the institutions encrypt sensitive data and the encryption keys are kept safe
- 50% have mechanisms to manage digital identities throughout their life cycle

- 66% do not have automatic password changes
- 83% have partially or fully implemented system session time out
- 50% are not using a single database for authentication across all systems
- 83% have fully implemented central anti-virus management
- 50% have their systems regularly check for updates on a central server
- 66% already have a backup strategy or are almost completing it
- 33% have their backup system include all major systems
- 66% have tested their backup for successful restoration

Overall, all institutions have the necessary ICT infrastructure (software and hardware) to form a base protection against information security attacks. As seen from the figure 4.2 below, most of the institutions except W achieved more than half the total points that could be accumulated by any one institution in this section. The observation is that while the institutions scored highly for possession of infrastructure, most of them lost points mainly around questions of implementation strategies.

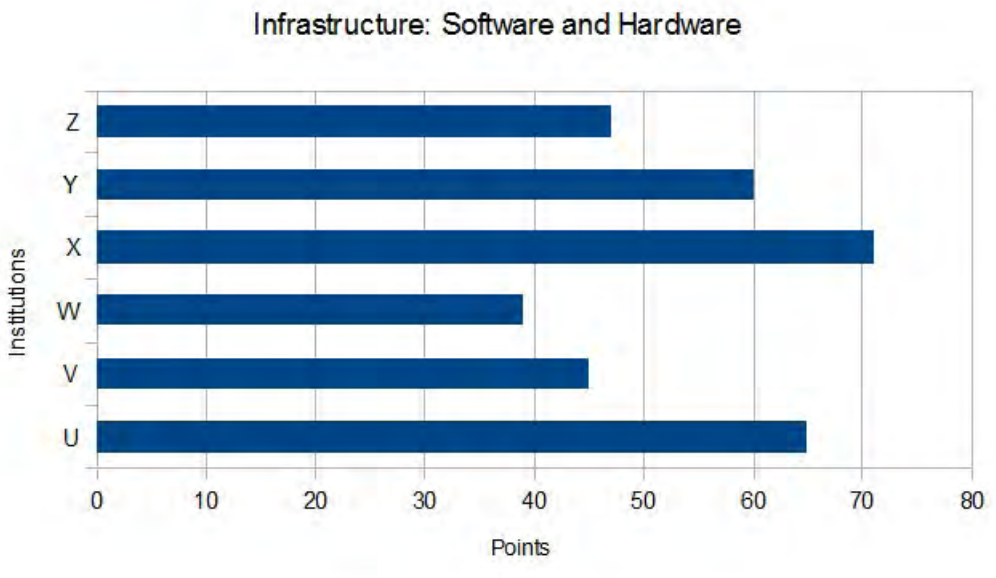

Figure 4.2: Infrastructure: Software and Hardware Summary

4.3 Human Resource and Awareness

Human resource and awareness was assessed using the staff composition for the ICT department and the ICT security awareness programs that an institutions has in place. This section answers the question *"What is the staff composition of the ICT department?"*

The table below shows the number of ICT staff in each of the institutions and the security-related qualifications that they have.

Institution	ICT Staff	Security Staff	Security Qualifications
U	15	3	Certified Network and Security Professional
V	30	0	Cyber Security Workshop attended
W	24	1	Offensive Security Certified Professional
X	4	1	None
Y	3	1	None
Z	5	1	None

Table 4.3: Summary: Staff Numbers and IT Security Qualifications

Two thirds of surveyed institutions indicated that they have an organised department whose role is to oversee the use of information technology resources on campus while the rest have "partially implemented" this or are "close to completion". Two thirds of surveyed institutions indicated that they have "partially implemented" the strategy to have a security function as one of the duties of the ICT personnel while the rest indicated they have "fully implemented" this and that their security function has the authority it needs to manage and ensure compliance with the information security program. All but one of the surveyed institutions indicated that they have made efforts to have ICT personnel train in security related courses
Two thirds of surveyed institutions ,when asked if they have an ICT security awareness program that caters for the whole institution, indicated "partial implementation" while the rest indicated "not implemented".

Two thirds of surveyed institutions indicated that their institutions do not carry out background checks on ICT employees while the rest indicated that they do carry out background checks.

Two thirds of surveyed institutions indicated that they have "fully implemented" data centres for their institution while the rest are working towards achieving this.

ICT Human Resource

It is important for any institution to have an ICT department whose role is to manage ICT resources that are on campus. These resources include computer terminals, servers, printers, telephone handsets etc. Having a single entity to manage all these resources makes one department accountable to all others for ICT services.

Having an ICT department is the first step to having an organised ICT environment. The second step is equipping it with staff who have the skill that mandate the work that the department oversees. The skills that are normally found in departments should include the director, database administrator, systems administrator, network administrator and support specialists, some roles merge the ones listed but these are the basic roles. All roles in the department should have the mandate to execute their duties, the security administrators role should be to oversee the departments execution of the ICT policy and its compliance by the staff members. It is important to note that all institutions have ICT departments which is a good sign. Also the numbers of staff in the departments varied but seemed to support the deduction that universities that have more user populations and have been in existence longer had more staff in the ICT departments than their newer and smaller counterparts.

ICT staff training is one of the responsibilities of the human resources department that should be implemented in order to equip the staff to face the ever changing ICT industry. The ICT field is continuously changing and universities are some of the entities that are normally at the fore front of this execution and implementation of cutting age ICT infrastructure. It is in the benefit of the university to keep staff up-to-date with the ICT trends.

Training should also include security-related training. Whether or not the institution has a dedicated security staff member, all staff should be able to undergo basic information security training. This kind of training does not only assist staff in detecting insecure procedures and practises but helps them interpret policy and be able to assist in its enforcement. For example, as much as some institutions had information security professionals on their teams, none had industry standard certifications like the Certified Information Systems Security Professional (CISSP).

4.3.1 Summary

- All institutions have either a fully functional ICT department or working towards one
- 33% of the members have an ICT security function
- 83% have taken their staff for ICT security related courses
- 66% have an on-going security awareness program
- 66% do not carry out background checks on their staff
- 66% have established data centres

Overall, more than half the institutions have an organised ICT department that is staffed with various professionals. As much as only one institution did not have a security professional among its staff, even those that did, have not equipped the security professional to carry out their duties. Also only one institution is currently doing background checks for their staff during the employment process.

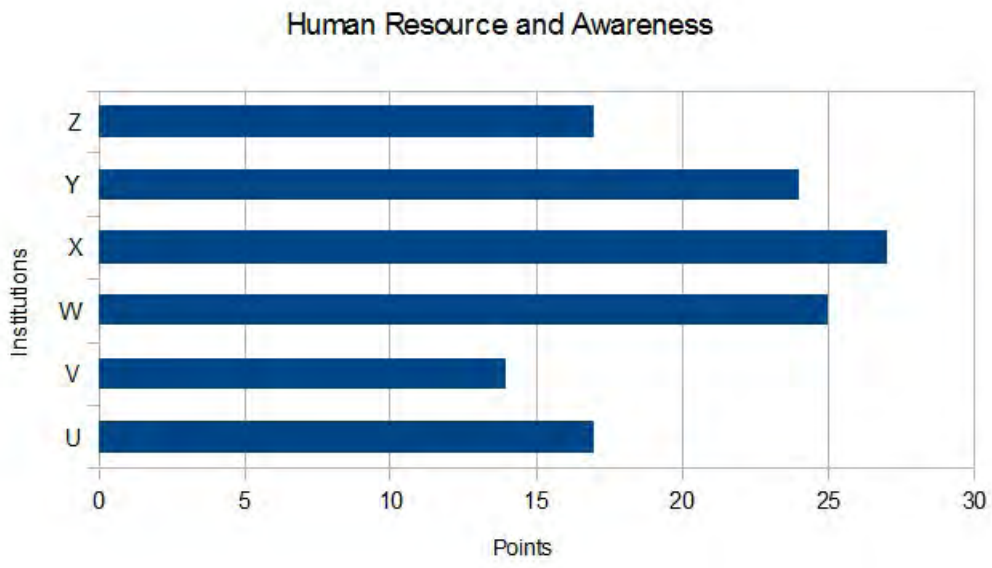

Figure 4.3: Human Resource and Awareness Summary

4.4 Policy

Policy was assessed using the existing policies that have been implemented by the ICT department and the measures taken to enforce policies and compliance. This section answers the question *"What Policies has the institution implemented to regulate Security and use IT resources?"*

- Two of the six surveyed institutions have already a published Acceptable use policy while three have "partially implemented" this. Only one institution is "close to completion". On ICT security policy, one institution indicated that are they have "not implemented" the publishing of their information security policy. The remainder are "close to completion" or have "fully implemented" this.
- One institution indicated that they have fully made the policies available to their users both students and staff while the rest have either "partially implemented" this or are "close to completion".
- Five of the institutions indicated that they have "partially implemented" or are "close to completion" on getting an effective way to communicate policy changes to users while the remaining one indicated that they have "fully implemented" this.
- Half of the respondents have fully communicated the consequences for non-compliance to their end users.
- Half of the respondents indicated that they do not include security-related clauses and sections with their external vendors while the remainder indicated that they are working to have this implemented.

4.4.1 Policy

A policy is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties [Michael and Herbert, 2010]. Policies can also be designed to be issue specific, for example information security policies are policies that are designed provide guidelines to protect information resources of an organisation.

It was good to note that all institutions either already have a published Acceptable use policy or are working towards one and many of the institutions are working towards getting their Security policies published. Policies are very instrumental in helping define

business goals and how the users of information resources in the institution are supposed to behave. Policies among other things can be used to control and or regulate the use of electronic resources such as the Internet, student data, confidentiality, illegal activities such as hacking and accessing pornographic sites [Fui-Hoon et al., 2002]. Policy designers should however, be careful to design policies that do not hinder staff from executing legitimate work but rather provide guidelines for responsible use of resources. Polices should also be as detailed as possible and leave no room for guessing intention during interpretation.
Policies especially security policies should also be designed to include external vendors, this is to protect the institution and its data in case the vendors come across confidential information. Involving vendors in awareness campaigns also helps vendor companies understand their role in the security of the institution and the consequences for non-compliance.

For policies to be successful, they must meet the following conditions:

Dissemination

Policies should be readily available to the staff of the organisation if they are to be put in practice. Changes to the policy must also be effectively disseminated [Fui-Hoon et al., 2002]. Possible ways of dissemination can include notice boards and electronically over organisation email lists. It was good to note that all institutions are already working on ways to disseminate their policies to their users. It should be noted that all institutions indicated the full understanding of this need and are all working towards devising best means of disseminating their polices.

Awareness

Management should be able to devise means of making their employees aware of the policy documents and their part in the overall picture of satisfying policy requirements. Awareness should be started by the employees fully understanding the institutions assets and why they should be protected. They should also understand the type of actions that can violate company policies for resources usage [Goetz, Johnson, and Pfleeger, 2009]. If the employees are aware of the assets and the need to protect them they are able to disarm any attempts made by attackers such as social engineering techniques.

Understandable

Policies should be understandable to all employees, if necessary they should be interpreted into various languages to make sure that the message cuts across the entire organisation. Management must make sure that all employees understand the contents of the policy, this can be done in form of group quizzes and puzzles.

Compliance

Policies should be very clear on the consequences for non-compliance and the penalties for each. It is also important that the penalties are the same across the board and enforced as directed by the policy. From the results, only 1/3 of the institutions have implemented this.

4.4.2 Data Classification

Two thirds of the surveyed institutions indicated that their policies do not classify the data that is stored on their servers and computers while one-third indicated that they are "close to completion" or have "fully implemented" this. Half of the surveyed instutitons indicated that their policies do not specify what kind of information about the institution can be taken home while the other half indicated that they are "close to completion" or have "fully implemented" this. On taking institutional devices home, two thirds of the surveyed institutions indicated that they do not have policies that specify who is allowed to take institutional devices off the institutions premises while one-third indicated that they have this "fully implemented".

Two thirds of the surveyed institutions indicated that they have "not implemented" or have "partially implemented" the strategy to specify how inter-department and office communication should be done while one-third indicated that they have "fully implemented" this.

Data Classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of data and documents is essential if you are to differentiate between that which is of less value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level.

For many organisations, a simple 5 scale grade will suffice as follows Top Secret, Highly Confidential, Proprietary, Internal Use only, Public Documents [Festus, 2008].

Data classification can greatly assist employees of the institution in the determining which documents they can share freely with other parties especially those who are not members of the institutions. it can also determine which kind of records can be taken off the institutions premises say to home for staff to continue working. Some of the documents that may pose serious security consequences are enrolment records, accounts records and students personal information.

4.4.3 Summary

- 33% have already a published Acceptable Use Policy (All have a document waiting approval).
- 83% are currently working on their information security policies.
- 16% have already made the policies available to their users.
- All institutions are either working or already have a way of disseminating policy changes to their users.
- 33% have communicated to their users consequences for non-compliance.
- 33% have included security-related clauses in vendor contracts.
- 33% have classified their data.
- 33% have their policies specifying what data can be taken home.
- 66% of the policies do not specify who is allowed to take devices off premises.
- 66% of the policies do not specify how inter-department communication should be done.

Overall, all institutions have an ICT policy written. However most of the institutions have not published their policies and have also not sensitized their users on the contents of the policies.

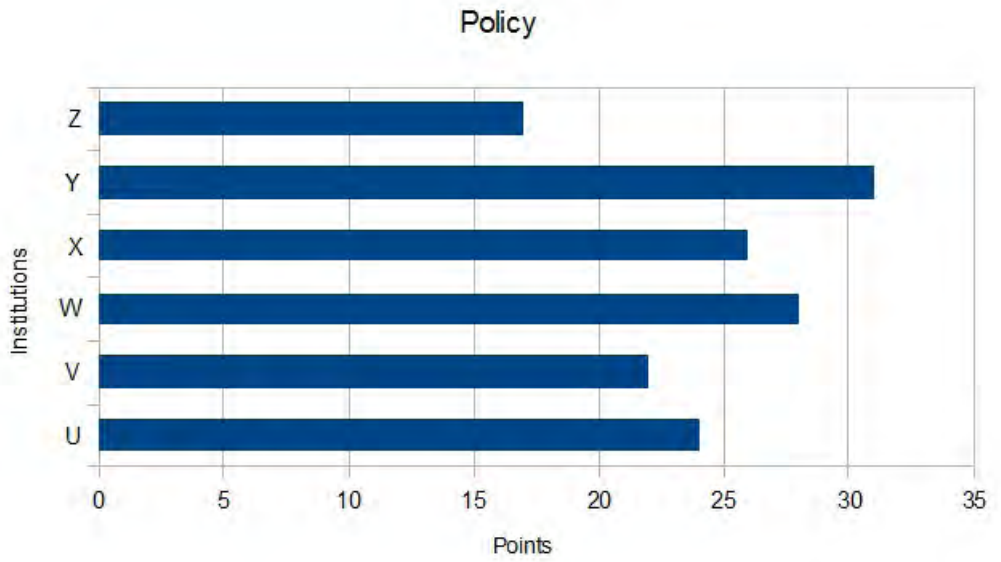

Figure 4.4: Policy Summary

4.5 Self Assessment

Self Assessment was assessed using common keywords used in information security to represent most common attacks and technologies. The respondents were asked to indicate their level of understanding of each of the terms. The respondents were also asked to rate the information security readiness of their institutions. This section answers the question *"How does the respondent access the institution's readiness to fight information security challenges?"*

The respondents were asked what their knowledge was of the most common security terms. These include "Firewalls", "Virtual Private Networks", "Botnets", "Intrusion Detection Systems", "Spyware", "Patching", "Rootkits", "VLANs", "0-days", "Anti-Virus Software", "Virii", "Malware", "DoS/DDoS", "SQL Injection", "Cross-Site Scripting", "Access Lists" and "Phishing".

All the respondents indicated that they fully understood what the terms "Firewalls", "Spyware", "VLANs", "Anti-Virus Software", "Virii", and "Malware" meant. This was expected as these are the common terms used in information security. It was concerning that none of the respondents knew about cross-site scripting and very few knew about SQL injection, 0-days and botnets. Figure 4.5 shows a representation of the different

words asked and the understanding of the respondents. Bigger sizes represent high level of understanding and vice-versa.

Figure 4.5: Representation of respondents understanding of security-related terms

Respondents were asked to rate the information security readiness of their institutions. The results are summarised in table 4.4.

Institution	**Readiness%**
U	60
V	80
W	80
X	80
Y	60
Z	45

Table 4.4: Respondents perceived security readiness of their institutions

Respondents were asked to share areas in information security that they think their institutions can improve on and these were the areas mentioned; VPN, Data back up, human resource awareness, policy, having an operational policy, enforcing standard security procedures such as authentication best practices, training of the line staff (IT section), centralized network access management, honouring the budget aspect, and regular IT audit.

4.6 Interview Questions

In this phase of the study, a pre-designed template was used to guide the interview session. The intention of the guide was to obtained more qualitative information on some of the

questions that were posed on the questionnaire. The guide was sent to the respondent in advance of the interview sessions so that the respondent could get a good grasp of the questions that were to be asked. All the interviews took place at the participating institutions premises. A tape recorder was used to capture the interview session so that the interviewer could be able to fully engage the respondent without having to transcribe as well. The following is a summary of the results collected during the sessions. The template used during this session can be found in Appendix B.

4.6.1 Changes with the Landing of SEACOM

All institutions identified a change with the landing of SEACOM. The landing of SEACOM at the East African coast provided easier access and cheaper bandwidth to East African countries and their Internet consumers. The institutions had their bandwidth doubled as was the the requirement from RENU for institutions to maintain their current expenditures on bandwidth so that subsequent reductions in bandwidth market prices continue to offer the institutions more bandwidth. Currently, among the participants in the survey the highest consumer of bandwidth is consuming 40mbps while the lowest is consuming 2mbps. Some institutions noted that with increased bandwidth, they have already added the number of computers to provide students with more access points to the Internet. Also it was noted that the numbers of students who own laptops increased significantly. This increase could can be attributed to the facts that reduction of Internet costs had made institutions able to provide more wireless points for student access and or that the governments waiver on taxes for computer equipment makes it easier for many students to afford laptops and other portable Internet ready devices.

4.6.2 Central Authentication Database

Only two institutions have implemented central authentication databases for their users. The first institution made use of Microsoft Active Directory, the second institution used Internet Message Access Protocol (IMAP) for authentication. The other institutions had not made any efforts to move in this direction. Central authentication is very crucial in an environment such as an academic institution. Academic institutions have many users ranging from staff to students, as well as guests that make use of the network and computer points available. Not being able to control who has access to which resources can be very dangerous since some users might use these resource to abuse systems on

the network or systems of other networks. Also centralising authentication helps in the management of user identities from creation to deletion. As a result users who have already left the institutions are unable to return and use institutional resources.

4.6.3 Campus Wireless Systems

Most of the institutions have a campus wireless system. Only one institution did not have a wireless system on campus. Among those that had wireless systems, the coverage range varied from 50 percent coverage to 100 percent coverage. Security implemented on the wireless systems varied from open access to MAC-address filtering to WPA and WEP encryption security. In general all institutions had grasped the need to have a way of controlling access to their networks over wireless LAN. None of the institutions had any means of knowing the number of users who were connected at a given time or whether all those who were connected were legally registered students and staff and not rogue users. All institutions had an offline method of knowing how many laptop users were registered to use the wireless system since access is only provided after registration.

4.6.4 Information Security Incidents

More than half the institutions had faced an information security incident in the past. The incidents seemed to indicate an insider threat. Incidents such as “an accountant changing accounts records” to “students changing results in the academic records system” and “a cleaner in the ICT department who was stealing server hard drives from a running server”. It is important to note that all incidents were noticed many weeks after they had occurred. Also during the course of this study two institutions experienced external security incidents. One institution’s website was hacked, another institution’s border gateway router was hacked and the running configuration erased. In both incidents, no post-incident auditing was performed so it is difficult to know whether they involved data loss or further attacks. On detection of possible on-going attacks, two institutions noted that they were able to detect if they were under attack by monitoring an Anti-Virus central logging dashboard and by monitoring server logs. However none of the institutions had a procedure to follow in order to mitigate such an attack if it were detected.

4.6.5 Blacklists

Half of the institutions public IP addresses had been blacklisted. Two of these institutions mentioned that the reason for the blacklist was as a result of virus activity on the network and the blacklist had been imposed by their upstream Internet providers. Their Internet connection service was stopped until the offending computers and subnets were discovered and isolated. The other institution that faced a blacklist was as a result of a user who shared the institution's credentials to access an online research journal with users on a torrent site and, as a result, the institutions credentials were being used by users in other parts of the world. The offended database shut down the institution's access to the database and a new set of credentials and guidelines were issued to the institution from the database's security administrators.

4.6.6 Physical Security

More than half the institutions reported a physical break-in into the ICT department. One of the institutions mentioned that "petty items" such as mouses, keyboards and monitors were stolen during the break-in while another noted that nothing was reported missing after the break-in. Another institution noted that the break-in led to the leaking of examinations. Only one institution mentioned that they had changed the office locks as part of the post-incident action. The rest of the institutions did not do any post-incident actions.

4.6.7 Operating Systems in use

All institutions were using a mix of Unix/Linux and Windows operating systems. It was found that Linux was mainly used as a server operating system for most of the institutions, although one institution used Linux as both its server and client operating systems. The favourite Unix/Linux distributions were FreeBSD, CentOS, Ubuntu and Fedora. The institutions that were running Windows on their clients were running a combination of Microsoft Windows XP, Windows Vista and Windows 2003 on their servers. Out of all the institutions, only one institution was actively patching their systems and auditing the patching process regularly.One other institution mentioned that the patching process is left to the individual users that make use of the computer while the rest of the institutions did not seem to do any managed patching at all.

4.6.8 Border Firewall use

More than half of the institutions are running border firewalls. However, of the institution that are running firewalls, none are performing any firewall auditing to make sure that the rules have not been changed and that the rules on their firewalls are running according to their policies. Of all the institutions running a firewall, only one had had the firewall implemented by a resident network administrator. The remaining institutions' firewalls had been implemented by former systems or network administrators and - in one case - had their firewall implemented by their Internet Service Provider.

4.6.9 IT Auditing

Only one institution had performed IT auditing in the past. The respondent from this institution mentioned that he remembered the audit from many years before but had never seen the report of the audit process.

4.7 Summary

This chapter presented the results and analysis of the data that was collected during the period of the research. It also included the responses of the interview sessions that were carried out with the respondents.
The following are some of the key findings that were discovered from the results of the study:

- Half of the institutions had between 401 – 800 staff and more than 5001 students.
- Half of the institutions spend between 10% – 20% of their ICT budget on information security related expenses.
- Half of the institutions were using more than three information systems including Financial Management Systems, Email Systems and Website Content Management Systems (CMS).
- 66% indicated that they employ third-party service providers such as software developers and that these providers do not go through secure recruitment processes.

- 66% of the institutions have not implemented a way to monitor their networks or to detect unauthorized use or rogue access points.
- 66% have already designed and implemented a back-up strategy. Of those, all have also tested the strategy for successful restoration.
- All institutions have a fully functional ICT department, although only 33% have an information security function within the ICT department.
- Only two of the institutions (33%) have already published an Acceptable Use Policy although only one has made this policy document available to their users.

Chapter 5

Conclusion

The purpose of this study was to investigate the information security practices put in place by the member institutions of Research and Education Network of Uganda (RENU) to safeguard institution information assets and systems from both internal and external security threats.

Although the initial study was to be conducted on all nine members of the Research and Education Network of Uganda, only six member institutions responded positively to take part in the study. As this was greater than half of the existing members, this researcher felt that the results obtained provide a valid overall picture of what is happening in the NREN and could be used to draw conclusions and offer recommendations to the NREN.

5.1 Research Overview

The following section offers the conclusions that have been drawn from the data collected. The conclusions are presented based on the research questions that were used during data collection.

5.1.1 *Research Question 1: "What is the institution's reliance on ICT systems and services?"*

The study found that the participating institutions were heavily reliant on ICT systems and services. This was exhibited by the fact that all institutions had already implemented

more than three information systems of those that were asked during the study including financial management systems, email systems and website management systems. Other indicators of heavy reliance on ICT systems included: the numbers of computing facilities available to staff and student use, availability of remote access systems (such as wireless systems), the perceived severity of system failure and loss of Internet connectivity to the institution (more than half of the institutions indicated that it would be critical to the proper functioning of the institution).

One indicator - "percentage of ICT budget spent on security" - that had been included on the questionnaire was not considered due to diversity in the financial management of ICT and security needs at the various institutions.. Some of the institutions spend on security related infrastructure from the central budget of the university while other institutions spend from the ICT department budget. In such cases it is difficult to clearly articulate the exact institutions' spending on security. Ignoring which budget is drawn from for security related expenditure, one key factor to note is that all but one institution spends on information security infrastructure. The exception made use of free, open source security solutions. Nonetheless, the heavy reliance on information systems in the universities that participated in the study is a strong indicator that these institutions should have a vested interest in ensuring their systems are protected from information security incidences.

5.1.2 *Research Question 2: "What IT security infrastructure has been deployed at the institution?"*

Based on findings of this study, institutions have already acquired and implemented some of the cutting edge equipment and systems, such as high-end border routers, and the latest operating systems, such as Linux and Microsoft Windows 7 and Server 2008. In addition, some of the institutions had already implemented more than one security layer such as gateway firewalls, application firewalls and anti-virus software on client machines. All institutions were found to have already implemented a backup strategy although none had tested their strategy to make sure it is effective.

As much as newer security technologies were found to be implemented at all institutions, the absence of guiding information security policies at the institutions meant that all these technologies were being implemented subconsciously and in so doing partially improving the overall information security posture. Because of the fast evolving global information security community, many makers of hardware and systems have hardened them for hostile

deployments such that by default some systems with no intervention of on-site security administrators are secure. A good example of such systems are the Windows 7 and Linux operating systems that have been designed by their vendors to be secure by default. Many of the institutions had the latest hardware, such as routers, and operating systems, such as Windows 7 and Windows Server 2008, which improved their overall security posture. None of these institutions, however, monitored these systems for abuse, nor whether they were adequately configured to defend the services they are running.

5.1.3 *Research Question 3: "What is the staff composition of the ICT department?"*

This question was asked in order to ascertain whether the institution had an ICT department and - in the event that it did - the kind of roles that exist in this department. According to the data collected, all institutions have an established ICT department that oversees the distribution of ICT services in the institutions. More than half the institutions have ICT staff whose responsibility is security of the institution's information assets. It was found that all security roles in the organizations were merged with other roles and, in addition, none of the staff were equipped with industry standard security qualifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or the Certified Information Systems Auditor (CISA) certifications. It was also found that none of the institutions carry out background checks before they hire ICT staff.

As discussed in the literature review, one of the challenges that institutions face when implementing information security practices is the lack of available information security staff. In John et al. [2003], the author mentions that universities are normally constrained to employ full time staff to run the security function of the ICT department. This was evident as no institution had a full time information security employee on the ICT team. The lack of a full time security employee hinders the security function since the employee who is assigned information security duties will have to juggle them with his other duties. With this revelation, it was no surprise that no institution had an ongoing information security program. According to [Lowendahl et al., 2006] the most-important step that an institution can take to strengthen its security efforts is the appointment of a Chief Information Security Officer (CISO). The document further stresses that the institutions should not stop at designating a CISO but should also give their newly appointed CISO the necessary mandate to drive the information security program.

5.1.4 *Research Question 4: "What policies has the institution implemented to guide students and staff on the proper use of ICT resources?"*

Based on findings from the study, all institutions have a written ICT policy, however few institutions published their policies. It was also found that institutions do not carry out policy sensitization and awareness campaigns for their staff and students. The composition of the policies was found to be lacking, with none of the institutions classifying how information should be handled in the institution. Also none of the institutions include security related clauses in their contracts with third-party service providers.

A number of studies Goetz et al. [2009] stress that policy should be the starting point of any information security program in any organization. In this case the absence of published information security policies not only means absence of information security programs at these institutions but also invalidate all attempts by institutions to implement information security practices. Nonetheless, even in the absence of a guiding policy, this study considered the various efforts made by the institutions to implement standalone information security practices as valid and commendable.

5.1.5 *Research Question 5: "How does the respondent assess the institution's readiness to fight information security challenges?"*

Respondents assessed that their institutions were ready to fight information security challenges. Most of the respondents felt that their institutions were 80 percent ready to fight information security challenges. Also from the results, the respondents had primary knowledge of information security and this could be seen from the security terms that they were able to identify. Users were able to identify and exhibit better understanding of terms such as "anti-virus", "firewall" and "spyware", but were not able to identify more advanced terms like "cross site scripting" and "SQL injection".

Despite the fact that respondents felt that their institutions were ready to fight information security challenges, other key indicators - especially lack of policy - suggested otherwise, as the security program of any organization can only be guided by its policy.

5.2 Validity of this Study and Results

The purpose of this study was to investigate the information security practices put in place by the member institutions of Research and Education Network of Uganda (RENU) to safeguard institutions' information assets and systems from both internal and external security threats. This document presented the results of the study. This researcher feels that the results are valid because of the following reasons:

5.2.1 Sample space

The research targeted all members of the Research and Education Network of Uganda. RENU, as a "young" NREN, only has nine member institutions out of the more than twenty institutions of higher learning that are in the country. The study obtained six positive responses from the contacted members, constituting more than half the members of the NREN at the time. As a result, it is believed that the results obtained from these members can be used to provide an accurate picture on the information security posture of the NREN.

5.2.2 Respondents

In the study participation invitation that was sent to institutions, this researcher asked the head of the various ICT departments to nominate an individual who had information on the security practices of the institution. Typically such an individual would be the Chief Information Security Officer (CISO). None of the institutions was found to have a CISO, so the heads of the institutions' departments nominated some other individual who they believed would be qualified to answer the questions. In some cases, the heads of department nominated themselves. In one instance a librarian answered the questionnaire as he is the head of department for ICT. Since the heads of department should be aware of the information security program, the information obtained from the respondents is deemed correct and a true representation of the institution's ICT security program.

5.2.3 Timing of the study

The study was meant to investigate the information security practices put in place by the member institutions of Research and Education Network of Uganda (RENU) to safeguard

institutions' information assets and systems from both internal and external security threats. Based on the title of the study, the researcher assumed that the universities had an information security program already in place and that the study would try to understand how it had been implemented, in addition to any merits they may have. It was discovered in the course of the research that none of the institutions had an ongoing security program. Nonetheless, since the institutions have standalone information security procedures in place, the researcher considers them major contributors to the overall security posture of the institution and therefore considers them valid indicators in the study.

5.2.4 Summary

The study on information security practices put in place by RENU member institutions to protect institution systems and data from security incidences discovered that institutions have not implemented appropriate practices and procedures to protect these systems and data. This conclusion is supported by the fact that none of the institutions have created nor published an information security policy. Policy is supposed to be the guiding tool that is used during the implementation of these procedures and practices. For example, all institutions were found to have cutting edge equipment and software systems implemented at their institutions. However, even with such advantages, these systems were not configured appropriately nor monitored for information security incidences, hence they did not perform optimally.

5.3 Future Research

The area of information security is still in its infancy in Uganda, in both industry and educational institutions. With the increase use of computing systems for both storage and access to information, it becomes a necessity for administrators of institutions to take information security seriously and implement information security controls to protect their systems and data.

- This study only focused on educational institutions that are members of the Research and Education Network of Uganda. In the case of Uganda, there are only nine universities that are currently members of RENU out of the over 20 universities that exist in the country. Future research work, especially if the members of the

NREN do not increase, could focus on all tertiary education institutions in order to get a clearer picture of the information security trends within education institutions in the country.

- Research on information security areas within National Research and Education Networks, especially on the African continent, are still not available. Future studies in this area could be beneficial for comparison purposes with results from other NRENs, especially within UBUNTUNet alliance which brings together NRENs in East and Southern Africa.

- In this study, the survey instrument that was used was customized from another tool that was originally developed by EDUCAUSE for the assessment of universities in the United States of America. Future studies could evaluate the possibility of designing a tool that could be used to evaluate security practises of NRENs on the African continent.

References

Rose-Mharie Ahlfeldt and Eva Söderström. Information Security Problems and Needs in a Distributed Healthcare Domain A Case Study. In *The Twelfth International Symposium on Health Information Management Research (iSHIMR 2007)*, pages 97–108, Sheffield, UK, July 18–20 2007. ISBN: 0 903422 40 3. URL `http://citeseerx.ist.psu.edu`.

O. B. Ajayi, A. S. Sodiya, and S. A. Ibrahim. The State of Information Security in South-Western Nigerian Educational Institutions. *Department of Mathematical Sciences*, 2004. URL `www.unaab.edu.ng/journal/index.php/COLNAS/article/download/174/172`. Retrieved September 6, 2011.

Robert Alai. Makerere University Website Haked. Online, 2011. URL `http://www.techmtaa.com/2011/06/07/makerere-universitys-school-of-computing-website-hacked/`. Retrieved September 6, 2011.

P Albertson, E. Thibeau Briana, Lohnes Dow, D. Salomon Kenneth, and C. Cassat Peter. IT Security for Higher Education, 2003.

Ndiwalana Ali. Challenges of Network Formation: Building the Research and Education Network for Uganda (RENU). Technical report, 2010. URL `http://www.uneca.org/istd/documents/EANRE/AliNdiwalana.pdf`. Online. Retrieved August 13, 2011.

Jon Allen and Jeff Wilson. Securing a wireless network. In *Proceedings of the 30th annual ACM SIGUCCS conference on User services*, SIGUCCS '02, pages 213–215, New York, NY, USA, 2002. ACM. ISBN 1-58113-564-5. doi: http://doi.acm.org/10.1145/588646.588696. URL `http://doi.acm.org/10.1145/588646.588696`.

H. Alvestrand, J. Hodges, R. Morgan, and M. Wahl. Authentication Methods for LDAP, 2000.

Rennie Archibald, Biswanath, Dipak Ghosal, Ken Chiang, Cherita Corbett, Yali Liu, and Mukherjee. Detecting sensitive data exfiltration by an insider attack. In *Proceedings*

of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, CSIIRW 08, pages 16:1–16:3, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-098-2. URL http://doi.acm.org/10.1145/1413140.1413159.

BBC News. East Africa gets high-speed web. Online, July 2009. URL http://news.bbc.co.uk/2/hi/africa/8165077.stm. Retrieved February 14, 2011.

BBUC. Bishop Barahm University College Website. Online, 2011. URL http://bbuc.ucu.ac.ug. Retrieved August 13, 2011.

Martin Beck and Erik Tews. Practical attacks against WEP and WPA. In *Proceedings of the second ACM conference on Wireless network security*, WiSec '09, pages 79–86, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-460-7. doi: http://doi.acm.org/10.1145/1514274.1514286. URL http://doi.acm.org/10.1145/1514274.1514286.

Williams Ben. Practical Steps to Wireless Networking in Schools. Online, 2004. URL http://download.microsoft.com/documents/uk/education/solutions/wireless/downloads/steps-wireless-networking-in-schools.doc. Retrieved September 9, 2011.

Eduardo Bertassi, Denis Gabos, Ian Korolkovas, Rodrigo F. Maia, Moacyr Martucci, Jr., and Edison Spina. A framework to mobility and interactivity for convergent technologies. In *Proceedings of the 5th WSEAS international conference on Multimedia, internet & video technologies*, MIV'05, pages 95–100, Stevens Point, Wisconsin, USA, 2005. World Scientific and Engineering Academy and Society (WSEAS). ISBN 960-8457-32-7. URL http://dl.acm.org/citation.cfm?id=1974548.1974569.

Steffani. A Burd, Scott. S Cherkin, and Joseph Concannon. Information Security in Academic Institutions Emerging Issues and Remediation Strategies. *Journal of Security Education*, 2005. URL www.ncjrs.gov/App/publications/Abstract.aspx?id=239613. Retrieved February 20, 2011.

Martin Campbell and William Aspray. *History of the Information Machine*. Harper Collins Publishers, 1999. URL http://computinghistorymuseum.american.edu/bookinfo/text3.pdf. Retrieved April 14, 2011.

Evan Cooke, Farnam Jahanian, and Danny McPherson. The zombie roundup: understanding, detecting, and disrupting botnets. In *Proceedings of the Steps to Reducing*

Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, SRUTI'05, pages 6–6, Berkeley, CA, USA, 2005. USENIX Association. URL http://dl.acm.org/citation.cfm?id=1251282.1251288.

Marcotte Cynthia. UCLAhealth systems payment of 865, 500*tosettleHIPAAchargesshowsrisingHIPA* //slphealthcareupdate.wordpress.com. Retrieved September 6, 2011.

Data Breaches. NCSU research info on Wilson students mistakenly put online, 2011a. URL http://www.databreaches.net/?p=20163.

Data Breaches. Security breach in april 2010 reported to affected purdue u. math students in 2011, 2011b. URL http://www.databreaches.net/?p=20167.

West David. EUMEDCONNECT a stimulus to the development of NRENs in North Africa. Online, 2005. URL www2.aau.org/tunis/presentation/proceedings.pdf. Retrieved September 9, 2011.

EDUCAUSE. Information Security Governance Assessment Tool. Online, 2005. URL http://net.educause.edu/ir/library/pdf/SEC0421.pdf. Retrieved August 22, 2011.

Mete Eminağaoğlu, Erdem Uçar, and Şaban Eren. The positive outcomes of information security awareness training in companies - a case study. *Information Security Technical Report*, 14(4):223–229, November 2009. ISSN 1363-4127. 10.1016/j.istr.2010.05.002. URL http://dx.doi.org/10.1016/j.istr.2010.05.002.

Entrust. Securing your digital life. Online, 2008. URL http://download.entrust.com/resources/download.cfm/21431/. Retrieved August 22, 2011.

Federo Register. Family Educational Rights and Privacy Act (FERPA). Online, April 2011. URL http://www.gpo.gov/fdsys/pkg/FR-2011-04-08/pdf/2011-8205.pdf. Retrieved September 5, 2011.

Olubukunmi Ajibuwa Festus. Data And Information Security In Modern Day Businesses. Master's thesis, Atlantic International University, 2008. URL http://www.aiu.edu. Retrieved September 27, 2011.

Dirk Fox. Zero Day Exploits. *Datenschutz und Datensicherheit DuD*, 33:250–250, 2009. ISSN 1614-0702. URL http://dx.doi.org/10.1007/s11623-009-0060-0. 10.1007/s11623-009-0060-0.

Fiona Fui-Hoon, Limei Nah, Teng, and Keng Siau. Acceptable Internet use policy. *Commun. ACM*, 45:75–79, January 2002. ISSN 0001-0782. URL `http://doi.acm.org/10.1145/502269.502302`.

Eiichiro Fujisaki and Tatsuaki Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 537–554, London, UK, UK, 1999. Springer-Verlag. ISBN 3-540-66347-9. URL `http://dl.acm.org/citation.cfm?id=646764.706343`.

Roy George, Max M. North, and Sarah M. North. Computer security and ethics awareness in university environments: a challenge for management of information systems. In *Proceedings of the 44th annual Southeast regional conference*, ACM-SE 44, pages 434–439, New York, NY, USA, 2006. ACM. ISBN 1-59593-315-8. http://doi.acm.org/10.1145/1185448.1185544 URL `http://doi.acm.org/10.1145/1185448.1185544`.

E. Goetz, M.E. Johnson, and S.L. Pfleeger. Security through Information Risk Management. *Security Privacy, IEEE*, 7(3):45 –52, may-june 2009. ISSN 1540-7993. 10.1109/MSP.2009.77.

Dieter Gollmann. *Computer Security*. John Wiley and Sons Ltd., West Sussex, United Kingdom, 2011.

M.I. Hasan and N.B. Prajapati. An attack vector for deception through persuasion used by hackers and crakers. In *Networks and Communications, 2009. NETCOM 09. First International Conference on*, pages 254 –258, dec. 2009. 10.1109/NetCoM.2009.59.

Kevin Henry. Getting started with PGP. *Crossroads*, 6(5), July 2000. ISSN 1528-4972. 10.1145/345107.345119. URL `http://doi.acm.org/10.1145/345107.345119`.

HHS Press Office. Massachusetts General Hospital settles potential HIPAA violations. Retrieved September 6, 2011, 2011. URL `http://www.hhs.gov/news/press/2011pres/02/20110224b.html`.

Sean B Hoar. Trends in Cyber Crime: THE DARK SIDE OF THE INTERNET. *Criminal Justice*, 20(3):4–13, 2005.

IHSU. International Health Sciences University, ISHU Website. Online, 2011. URL `http://www.ihsu.ac.ug`. Retrieved August 13, 2011.

Internet2. About Internet2. Online, www.internet2.edu/about/faq.html, 2008. URL `www.internet2.edu/about/faq.html`. Retrieved August 13, 2011.

Dyer John. Developing the Case for NRENs. In *TERENA*, 2008. URL `http://www.terena.org/events/pdfs/nren-case-v1.ppt`. Retrieved August 13, 2011.

Voloudakis John, B. Caruso Judith, A. Pirani Judith, King Paula, B. Kvavik Robert, and N. Katz Richard. Information technology security: Governance, strategy, and practice in higher education. *ECAR Research Study*, Vol. 5, 2003.

Dr. Javed I. Khan. BDREN and A New Era in Bangladesh Higher Education. Online, 2008. URL `http://www.medianet.kent.edu/techreports/TR2009-01-ICCIT2008-BdREN.pdf`. Retrieved August 13, 2011.

Brett J. L. Landry and M. Scott Koger. Dispelling 10 common disaster recovery myths: Lessons learned from hurricane katrina and other disasters. *J. Educ. Resour. Comput.*, 6, December 2006. ISSN 1531-4278. http://doi.acm.org/10.1145/1248453.1248459. URL `http://doi.acm.org/10.1145/1248453.1248459`.

Homin K. Lee, Tal Malkin, and Erich Nahum. Cryptographic strength of ssl/tls servers: current and recent practices. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, IMC '07, pages 83–92, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-908-1. 10.1145/1298306.1298318. URL `http://doi.acm.org/10.1145/1298306.1298318`.

Jan-Martin Lowendahl, Marti Harris, and Michael Zastrocky. Best Practices for Justifying and Allocating Higher Education Security Resources, February 2006. URL `http://confluence.arizona.edu`.

E. Whitman Michael and J. Mattord Herbert. *Principles of Information Security, 3rd Edition*. Course Technology. Cengage Learning., 2010.

Missouri State University Press. College of education students notified of security breach. Online, 2011. URL `http://news.missouristate.edu/2011/03/03/coe-security-breach/`. Retrieved September 7, 2011.

Robert Morris and Ken Thompson. Password Security: A Case History. *Communications of ACM*, 1979. URL `https://info.aiaa.org/tac/isg/SOFTC/PublicDocuments/TechnicalWorkingGroups/CyberSecurity/PasswordSecurityAcaseStudy.pdf`.

MUBS. Makerere University Business School, MUBS Website. Online, http://www.mubs.ac.ug, 2011. URL `http://www.mubs.ac.ug`. Retrieved August 13, 2011.

MUK. Makerere University Website. Online, 2011. URL `http://www.mak.ac.ug/`. Retrieved August 13, 2011.

MUST. Mbarara University of Science and Technology, MUST Website. Online, 2011. URL `http://www.must.ac.ug`. Retrieved August 13, 2011.

NCP Website. National Cyber Security Partnership website. Online, 2003. URL `http://www.cyberpartnership.org`. Retrieved August 22, 2011.

Chiwaraidzo Judith Nyabando. *An analysis of perceived faculty and staff computing behaviors that protect or expose them or others to information security attacks*. PhD thesis, East Tennessee State University, 2008. AAI3323685.

Ohio University Press. Ohio state notifies of unauthorized access to university server, 2010. URL `http://www.osu.edu/news/newsitem2985`. Retrieved February 21, 2011.

Oaiya Omo. West and Central African Research and Education Network (WACREN). *EURO- AFRICA WEEK ON ICT RESEARCH & E-INFRASTRUCTURES*, 2010. URL `http://euroafrica-ict.org`. Retrieved September 29, 2011.

Parliament Of Uganda. THE COMPUTER MISUSE BILL. Online, 2008. URL `http://www.parliament.go.ug/billtrack/bills/text/2008-023.doc`. Retrieved September 6, 2011.

N. Pavkovic and L. Perkov. Social Engineering Toolkit 2014; A systematic approach to social engineering. In *MIPRO, 2011 Proceedings of the 34th International Convention*, pages 1485 –1489, may 2011.

P Piassa. CDW G Higher Education IT Security Report Card 2006. *CDW Government*, 2006. URL `http://newsroom.cdwg.com/features/HEITSecurityReportCard10-10-06.pdf`. Retrieved February 20, 2011.

Encarnacion Pyle. The Columbas Dispatch. *http://www.dispatch.com*, 2010. URL http://www.dispatch.com. Retrieved February 21, 2011.

RENU. Memorandum of Understanding Of the Research and Education Network for Uganda, 2006. URL http://www.renu.ac.ug/publications/01--inaugural/renu--mou.pdf. Retrieved August 13, 2011.

RENU. RENU Website. Online, http://www.renu.ac.ug, 2011. URL http://www.renu.ac.ug. Retrieved August 13, 2011.

Koen Schelkens. TERENA TF- Work area NREN Service Portfolios. *BELNET*, 13, 2006. URL http://www.terena.org/activities/tf-msp/nren-service-cats.pdf.

Secunia. Secunia half year report 2010. Online, 2010. URL http://www.secunia.com/gfx/pdf/Secunia--Half--Year--Report--2010.pdf. Retrieved September 6, 2011.

Malcolm Shore, Du Yi, and Sherali Zeadally. A Public-Private Partnership Model for National Cybersecurity. *Policy and Internet*, 3, 2004. URL http://www.psocommons.org/policyandinternet/vol3/iss2/art8. Article 8.

Philip Spohn. Happy Trails Computer Club. Online, 2011. URL http://cybercoyote.org/security/av-top.htm. Retrieved September 6, 2011.

Song Steve. African Undersea Cables. Retrieved September 6, 2011, 2011. URL http://manypossibilities.net/african-undersea-cables/.

Alex Twinomugisha. Understanding NRENs and Key Considerations while establishing them. Online, 2007. URL http://www.gesci.org/old/files/NationalResearchandEducationNet
pdf.

UCU. Uganda Christian University, UCU Website. Online, 2011. URL http://www.ucu.ac.ug. Retrieved August 13, 2011.

UNESCO. The International Association of Universities (IAU). Online, 2009. URL http://www.unesco.org/iau/onlinedatabases/list--data/u-nw.html. Retrieved September 6, 2011.

U.S. Department Of Justice. Student Charged with Using University Computer Network for Denial of Service Attacks, 2010. URL `http://www.justice.gov/criminal/cybercrime/frostChar.pdf`. Retrieved February 28, 2011.

Karel Vietsch. *Creative and innovative network management*, pages 27 – 36. Computer and Systems Sciences. IOS Press, 2003.

Kenneth A Williams, Omari T. Wright, Xiaohong Yuan, and Huiming Yu. Laboratory design for wireless network attacks. In *Proceedings of the 5th annual conference on Information security curriculum development*, InfoSecCD '08, pages 5–12, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-333-4. http://doi.acm.org/10.1145/1456625.1456629. URL `http://doi.acm.org/10.1145/1456625.1456629`.

Kadzamira Zimani. UbuntuNet Alliance and NRENs. Online, 2007. URL `http://www.malico.mw/maren/docs/ubuntunet--vc.pdf`.

Appendix A

Consent Form

RHODES UNIVERSITY

CONSENT FORM
Department of Computer Science

Project Title: An Investigation into Information Security Practices implemented by Research and Educational Network of Uganda (RENU) Member Institutions

Researcher's names: Researcher: Alex Kisakye Supervisor: Dr. Barry Irwin

---

- I have received information about this research project.
- I understand the purpose of the research project and my involvement in it.
- I understand that I may withdraw from the research project at any stage.
- I understand that participation in this study is done on a voluntary basis.
- I understand that while information gained during the study may be published, I will not be identified and my personal results will remain confidential.
- I understand that I will receive no payment for participating in this study.

Name:.....

Signed ..... **Date** .....

I have provided information about the research and believe that participant understands what is involved.

Researchers signature and Date.....

Appendix B

Interview Guide

Proposed Interview Questions.

1. Did you notice a change in the utilization of computing resources with the landing of the SEACOM cable? Please give details.
2. Are you using the same database for authentication across all application systems? If yes, which vendor authentication database is used?
3. If a campus-wide wireless system is available, what is its coverage? What security has been implemented on it? Do you know the number of users allowed to use the wireless system?
4. Do you have means of knowing characteristics of the users using the wireless network at any time e.g. numbers, legitimate users
5. Have you experience an information security (IS) incident before? Please give details.
6. Do you have means of knowing in real-time if you are under attack?
7. Do you have a procedure to follow once and IS attack has been detected?
8. Has any of your public IP address space been blacklisted before?
9. Can you describe how the reason for the blacklist was discovered and how it was remediated?
10. Have you had any information security incidents in your department before? What type of incidences were they? How were they discovered? Where any measures taken post-discovery to prevent future attacks?
11. What are the biggest security threats to your systems? How have you responded to prevent such threats from happening?
12. Has your department ever been physically broken into? How was the break-in discovered? Did you manage to find anything missing after this incident?
13. Do you have a disaster recovery plan? Who is responsible for administration and coordination of the plan? Where is the disaster recovery plan stored? Do you have an offsite backup location? Have you ever had to use the backup plan? If yes please describe the incident that let to its use.
14. Do you have an intuition-wide anti-virus? How regularly do the clients update their virus databases? Does someone regularly check the AV providers' site to discover new known viruses?
15. What operating systems does the institution use for desktops and servers? How is patching managed? Do you actively look at vendor sites for new vulnerabilities? Do you actively audit system patching process?
16. Do you use a border firewall? Who implemented the firewall? Who is responsible for making necessary changes? Is there a policy that determines what kind of traffic to let through or block? Are the changes on the firewall authorized and documented? Are the firewall rules regularly audited for consistency with the documentation?
17. Do you carry out an audit of your IT systems? If yes, is the auditing done in-house or by a third-party service provider? If you are using a third party provider, have you taken the necessary procedures to have a non-disclosure agreement? How often is the auditing done?
18. Are all public facing systems like website regularly monitored for consistency? Are the webserver logs monitors for any unexpected behavior?
19. Do you have an Acceptable use policy? Do you have an information security policy? Are copies of these documents readily available to your users? Have these documents been mandated by

top management? Do the documents clearly specify which resources are to be protected? Do the documents clearly mention the consequences for non-compliance?

20. Are staff allowed to take off campus university equipment and information?

Appendix C

Survey Questionnaire

Questionnaire

Role of Respondent in the organization……..

SECTION 1 **Institutional Profiling** This section assesses the Institutions' reliance on Information Technology systems and services.		
1.	**Select Appropriate score [A, B, C etc.] and filling the score section.**	**Score**
1.1	What is your average annual ICT budget (in UGX)? Less than 100Million = A 101Million to 300Million = B 301Million to 600Million = C 601Million to 1Billion = D 1Billion and over = E	
1.2	What is your annual average spending on Security related services and products? E.g. Anti-virus, IDS etc. 0 = A 1Million to 20Million = B 21Million to 50Million = C 51Million to 150Million = D 151Million to 300Million = E 301Million and over = F	
1.3	What is the; number of staff institution-wide? 1 – 200 = A 201 – 400 = B 401 – 800 = C 801 – 1600 = D 1601 – 3000 = E 3001 and over = F	
1.4	number of Students? 1 – 500 = A 500 – 2000 = B 2001 – 5000 = C 5001 – 15000 = D 15001 – 40000 = E 40001 and over = F	
1.5	number of computers connected to the internet (both available to staff and students)? Less than 100 = A 101 – 300 = B 301 – 800 = C 801 – 1500 = D 1501 – 3000 = E 3001 and over = D	

1.6	Please select all the systems that your institution uses.	Select all that apply [**X** or **√**]			
	Academic Records Management Information System				
	Financial Management System				
	Students Management System				
	Library Information System				
	Learning Management System				
	Alumni Management system				
	Email System				
	Website System (content management system)				
	Other systems				
	Impact Assessment of System failure or loss of internet connectivity (Note scoring, A=None, B=Partial, C=Critical, D=Unacceptable				
1.7	What is the impact of system failure on the following	A	B	C	D
	i.) Internal Business processes of the institution (e.g. Registration)?				
	ii.) Business process between the university and external sources?				
	What is the impact of loss of internet connectivity on the following	A	B	C	D
	i.) Internal Business processes of the institution (e.g. Registration)?				
	ii.) Business processes between the university and external sources?				
1.8	Do you contract third party entities for any of your business processes (e.g. software development, network expansions)? YES NO				
1.9	Do you have persons that work in the offices but are not on the Institutions' Payroll system (e.g. office-helps, cleaners, interns)? YES NO				
1.10	Does your institution have a wireless access system for staff and student device access? YES NO				
1.11	If you answered yes in 1.7, what encryption is in use? No Encryption = A WPA = B WEP = C				
1.12	Do you provide for staff and students a means to access university systems remotely? YES NO				

Section 2:
Infrastructure: Software and Hardware

This section assesses the current Security Infrastructure that has been deployed by the Institution.
Grading for this section is as follows;
A= Not implemented, B =Partially Implemented, C= Close to Completion, D = Fully Implemented

2.1	Are internet-accessible servers protected by more than one security layer? (firewall, network IDS, Application IDS)	
2.2	Are your networks, systems, and applications periodically scanned to check for vulnerabilities as well as integrity of configuration files?	
2.3	Do you constantly monitor in real time your networks, systems and applications for unauthorized access and anomalous behaviors such as viruses, malicious code insertion, or break-in attempts?	
2.4	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	
2.5	Is sensitive data encrypted and associated encryption keys properly protected?	
2.6	Are there effective and reliable mechanisms in place to manage digital identities (user accounts, keys, tokens) throughout their life-cycle, from registration through termination?	
2.7	Do all of your systems and applications support and enforce automatic password change management or automatic expiration of passwords, as well as password complexity and reuse rules?	
2.8	Do your systems and applications enforce session/user management practices including automatic timeouts, lockout on login failure, and revocation?	
2.9	Do you employ specific measures to prevent and detect rogue access for all of your wireless LANs?	
2.10	Do you employ specific measures to secure remote access to your servers?	
2.11	Do you employ specific measures to secure the servers that manage your network domain names and addresses (DNS and DHCP servers)?	
2.12	Is every workstation and server protected with centrally managed anti-virus?	
2.13	Is there an audit trail to verify that virus definitions files are updated frequently and systematically?	
2.14	Is every desktop workstation and server updated regularly with the latest operating system patches from a central update server?	
2.15	Taking into account severity and urgency, are there mechanisms in place to report and respond to a variety of anomalies and security events?	
2.16	Is there a current system backup strategy?	
2.17	Does the backup strategy cover all critical systems in the institution?	
2.18	Are the backup procedures periodically tested to make sure recovery is possible?	
2.19	Are all system configuration changes done according to policy and the changes documented?	
2.20	Do all your applications have a central database for authenticating users (e.g. LDAP)?	

Section 3:
Human Resource and Awareness:

This section assesses the human resource component of the Institutions Information Security resources.
Grading for this section is as follows;
A= Not implemented, B =Partially Implemented, C= Close to Completion, D = Fully Implemented

3.1	Does your institution have an organized ICT department whose role is to oversee the use of Information technology resources?	
	How many staff are in your ICT department? ……	
3.2	Is there a security function in any of the duties of ICT personnel (independent or merged)?	
	How many staff are assigned to the security function in your department? ……	
3.3	Does your information security function have the authority it needs to manage and ensure compliance with the information security program?	
3.4	Does your information security function have the resources it needs to manage and ensure compliance with the information security program?	
3.5	Is there effort to train ICT personnel in security related courses?	
3.6	Do ICT personnel have ICT security qualifications? If yes please list them below. a.) b.) c.) d.)	
3.7	Do you have an ICT security awareness program that caters for the whole institution?	
3.8	Does your institution carry out background checks on ICT employees e.g. check out references of the employees that are hired to perform ICT functions?	
3.9	Do you have a central place where all institutions' systems are stored (i.e. server room, data center)?	

Section 4: **Policy:** This section assesses the Institutions' policy on usage of the ICT resources and services. Grading for this section is as follows; A= Not implemented, B =Partially Implemented, C= Close to Completion, D = Fully Implemented		
4.1	Does your institution have a published Acceptable Use Policy?	
4.2	Does your institution have a published Information Security policy?	
4.3	Are the policies readily available to your users [students and staff]?	
4.4	Do you have an effective means of communicating policy changes to your users?	
4.5	Are the consequences of non-compliance clearly communicated and enforced?	
4.6	Are relevant security policies included in all third-party contracts?	
4.7	Do the relevant policies classify the data and information that is stored on the systems or shared between departments (e.g. confidential, sensitive)?	
4.8	Do the relevant policies specify what kind of data or information about the institution can be taken home by staff members?	
4.9	Do the relevant policies specify who is allowed to take institutional devices off the institutional premises (e.g. Laptops)?	
4.10	Do you have policies and procedures that describe how inter-department and office communication should be done?	

Section 5:

Self-Assessment:

This section assesses the respondents knowledge of some of the terms from Information Security field.
Grading for this section is as follows;
A= Don't Know, B =Not Sure, C= Know about it, D = Fully Understand

5.1	The following terms are from the Information Security field; please indicate your understanding of each term.	
	Firewall	
	Virtual Private Network	
	botnet	
	Intrusion Detection System	
	Spyware	
	Patching	
	rootkit	
	VLAN	
	Patching	
	0-day	
	Anti-Virus	
	Virus	
	Malware	
	Denial of Service /Distributed Denial of Service	
	SQL injection	
	Cross Site Scripting	
	Access Lists	
	Phishing	
5.2	On a scale of 0 - 100%, How would you describe the level of Information security readiness of your institution?	
5.2	Can you think of areas that you need to work on as an Institution to improve your Information security readiness.[Please use separate sheet if necessary]	