LESSONS LEARNT IN THE PROCESS OF COMPUTERIZATION, AUTOMATION AND MANAGEMENT OF ICT SECURITY IN THE DEVELOPING WORLD: A CASE STUDY OF THE UNIVERSITY OF DAR ES SALAAM, TANZANIA

Geoffrey Karokola[1] and Louise Yngström[2]

Department of Computer and System Sciences Stockholm University/Royal Institute of Technology
Forum 100, SE-164 40 Kista, Sweden Tel: +46 (0)8 16 1697, Fax: +46 (0)8 703 90 25 E-mails: {karokola1, louise2}@dsv.su.se

ABSTRACT
This paper intends to discuss and sift out current and important challenges in Information and Communication Technology (ICT) security for developing countries in the Sub-Saharan Africa where Tanzania will be taken as a case study. As a background we analyze lessons learnt in the processes of computerization, automation and the management of ICT security at the University of Dar es Salaam (UDSM) since it is one of the first higher learning institutions in Tanzania. The backbone of UDSM currently connects more than three thousand workstations and twenty five heavy duty servers that are centrally managed and which support different institutional core services.

In the evolution process of computerization and automation of Information and Communication Technology (ICT) at the UDSM that started way back in the early 1990's ICT security was of no priority. While in the western world computerization and automation processes have gradually been incorporating security into ICT infrastructures, developing countries have not experienced a similar evolution – neither in technical nor in practical circumstances. In practice, developing countries need to conform to international developments within ICT security at the same time as they are trying to conform to their own environments and also learn about

the totally new situation created. Simultaneously there are also local and specific restrictions – well known by the developing countries -but usually not experienced by the developed world.

KEY WORDS
Challenges, Lessons learnt, ICT Security, Information Security, Automation, Computerisation, Managing, Developing World

LESSONS LEARNT IN THE PROCESS OF COMPUTERIZATION, AUTOMATION AND MANAGEMENT OF ICT SECURITY IN THE DEVELOPING WORLD: A CASE STUDY OF THE UNIVERSITY OF DAR ES SALAAM, TANZANIA

1 INTRODUCTION

Information and Communication Technology (ICT) is considered to be a major driving force of globalised and knowledge based society in a modern world. As technology remains dynamic, protection of information asserts has became very challenging. A number of attacking techniques exists including denial of service attacks, cross site scripting, content spoofing, phishing, man-in¬the-middle, and brute-force. Therefore, proper protection of information assets in ICT infrastructures is needed. ICT security is considered to be part of that, where confidentiality, integrity and availability to information assets are the three pillars of major concern.

In developed countries the evolution process of computerisation and automation of ICT infrastructures gradually integrates ICT security. However, staring from early 1990's most of developing countries, particularly sub-Saharan Africa has experienced hasty un-secure evolution processes in computerisation and automation of ICT infrastructures [1]. There are critical factors in the developing world that negatively influence the process including lack of awareness and security culture, lack of knowledgeable and experienced human resources in managing ICT facilities, and un-secure integration of ICT security. While in the western world computerization and automation processes have gradually been incorporating security into ICT infrastructures, developing world has neither technical nor practical experience in similar evolution. As a result many organisation and institutions in developing world experienced losses of potential synergies [2, 3].

In this study, University of Dar es Salaam (UDSM) being one of the key player in ICT security in Tanzania and one of the first and leading higher learning institutions is taken as a case study. Furthermore, we

analyze and sift out challenges and lessons learnt in the processes of computerization, automation and managing ICT security at UDSM.

The paper is organised as follows: the background to the studied environment and an ICT security overview in Tanzania is given in chapter one; chapter two presents methodology; chapter three presents ICT security implementation status, chapter four presents challenges and counter¬measures; chapter five presents discussion and lessons learnt. Lastly conclusion and recommendations are given in chapter six.

1.1 Background to the Studied Environment

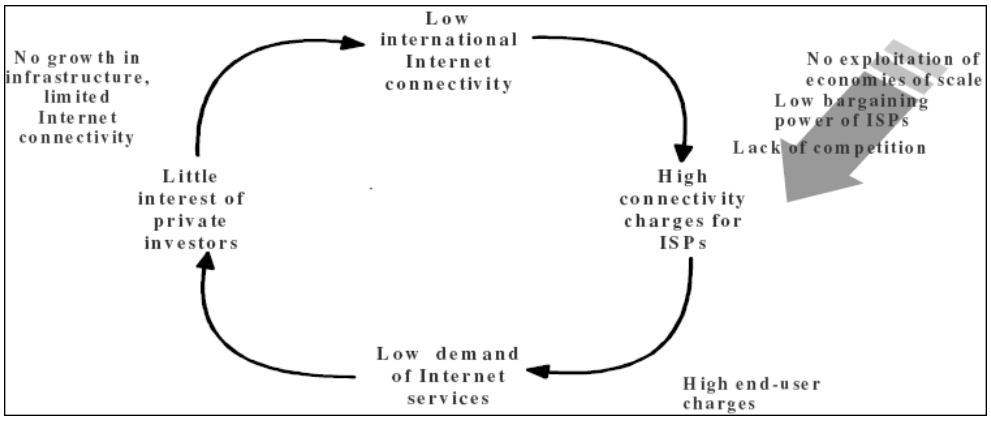
The University of Dar es Salaam (UDSM) is one of the first and leading public higher learning institutions in Tanzania. UDSM was firstly established in 1961 as an affiliated college of the University of London. In 1963 UDSM become the constituent college of University of East Africa and in1970 an independent university [1, 7, 12]. The primary objectives of UDSM were: to transfer knowledge from one generation to another; to establish a place in Tanzania where frontiers of knowledge would be advanced through research; and to be a place where professional training of human resource would be conducted [1, 7, 9]. The university started with only one faculty, the faculty of Law. Gradually it expanded to include more than five campuses; six faculties, four centres, and four institutes – at the main campus alone; and two constituent colleges [1, 7, 12]. In terms of student's enrolment, in 2006/2007 the university has a total of 18,342 students with females constituting 36.1% of all undergraduates [5].

The computerization, automation and integration of ICT security process at the university started in the early 1990's. Apart from many challenges posed as a result of this process over 16 years (1990's – 2007), great achievements were realised -as it is presented and discussed in the paper. The university recognition in offering high quality education and related ICT-based services is recognised amongst the African countries; in the African Universities ranking of 2005 conducted by Webometrics Ranking of World Universities: Cybermetrics Lab, National Research Council, Spain, UDSM appeared to be in the thirteenth position using ICT for teaching and learning [14]. All ICT-based services at UDSM are centrally coordinated and managed by the University Computing Centre (UCC) [1, 7, 9].

1.2 ICT Overview in Tanzania

Confidentiality, Integrity and service Availability are the three pillars for ICT security and special attention needs to be paid to bandwidth being one of the major contributing factors. In most African countries the internet connectivity to the outside world is satellite dependent. As a result of bandwidth charges in Africa being very high, automatically the integration of ICT security in universities and quality service delivery is highly affected [15].

According to the International Telecommunication Union (ITU) report, they argue that higher bandwidth prices in African countries are notably influenced by certain bottlenecks elements. Lack of infrastructures, unfavourable regulatory environment, and uncompetitive market structure were mentioned as influencing elements [4]. The report also gave the economics and consequences of high bandwidth prices to end-users, which are summarised and presented in the figure below.



Source: ITU report on improving IP connectivity in the least developing countries [4]

From these facts, it is obviously that with the existing wider economical gap between developing and developed countries, these higher bandwidth charges are unaffordable, and widens the digital divide. Cheaper and affordable bandwidth is necessary for African HEI's to excel.

The government through the Ministry of Communication and Transport (MoCT) and Tanzania Communications Regulatory Authority (TCRA) formally Tanzania Communication Commission (TCC) is also

advocating availability of cheaper and affordable bandwidth where as regulations permit international VSAT data service providers [2, 6]. To-date Tanzania has a total of fifty-three registered ISP's companies: eight companies with Network Facilities Licenses; eight with Network Service Licenses; and thirty-seven with Application Service Licenses [6]. These ISP's are offering internet services via VSATs', Wireless, leased lines, and dialup.

With regards to computers, the importation of ICT facilities, including computers started in early 1970's. However, there were a number of problems associated with operations, maintenance and management of ICT facilities. As a result the government experiences heavy financial losses. To stop the losses in 1974 the government decided to ban the importation of computers and its related equipments [2]. In early 1980's the ban were lifted. Most of computers and ICT related facilities were then imported by the government, private companies and few individuals [3]. In order to promote the growth, use and affordability of ICT facilities in the country, in early 2000 the government decided to wave taxes to the importation of computers. Since then the dependences on ICT to operate core services in all sectors increased hasty. Similarly status of ICT security awareness among people and its integration to support core business is fairly high.

2 METHODOLOGY

The study is based on the literature review, research work and findings from the four PhD graduates on ICT security paradigm in the studied environment [3, 8, 10, 11]. The study also grips authors working experience of nearly ten years as a forefront in the implementation and management of ICT security in the area.

3 ICT SECURITY IMPLEMENTATION STATUS

This chapter presents UDSM ICT-based services growth trends over the span of nearly sixteen years (1990's -2007) and how ICT security was integrated in the evolution process.

3.1 ICT Network Infrastructure and its Facilities

Having a secure, reliable, and well managed ICT network infrastructure in any organisation is a necessity for high quality service delivery. Security mechanisms including intrusion detection systems (IDS), firewalls, routers,

and virtual LAN (VLAN) are used to secure network infrastructures from attackers who exploit network vulnerabilities.

UDSM being the place where professional training of human resource is conducted -was not left out in ICT development arena. During 1990's – 2007 university progressively implemented the state of the art ICT network infrastructure that consists of gigabit speed optical fibre backbone, wireless links, and structured LAN's at UDSM main campus, constituent's colleges and at its institutes (UCLAS, MUCHS, DUCE and IJMC)[1]. To enhance distance learning -videoconferencing facilities were also installed [1, 7, 9, 12, 17]. Some of the areas covered in the process were:

- Optic fibre backbone: all buildings, including student's halls of residence and Public access Rooms (PAR)[2] at UDSM main campus were linked to the university optical fibre backbone. Also UDSM backbone was extended to UCLAS located more than 2km from the main campus. Optical fibre backbone(s) were also installed at UCLAS, MUCHS, and DUCE.
- Point to point wireless link networks: Other institutes and hall of residents (MUCHS, DUCE, IJMC and Mabibo hostel) located far from the UDSM main campus were connected to UDSM backbone via wireless microwave links with 11-23Mbps capacity.
- Wireless Access Points (Wi-Fi): Both outdoors and indoors WPA's were installed at the UDSM main campus and DUCE for creating flexibility and mobility to staff and students.

---

[1] UCLAS - University College of Lands and Architectural Studies; MUCHS - Muhimbili University College of Health Sciences; DUCE - Dar es Salaam University College of Education; IJMC – Institute of Journalism and Mass Communication.

[2] Rooms located to the student's halls of residence providing ICT related services to students; services include internet access and printing.

- Videoconferencing: Four UDSM main campus lecture theatres were installed with video conferencing facilities, and two sets of mobile facilities are available for use. However, in the process ICT security implementation and integration to automated services were observed to be of ad-hoc character. To-date UDSM backbone network infrastructure is believed to be one of the best heterogeneous network in higher learning institutions in eastern Africa.

3.2 Computers and its Facilities

Existing state of the art network infrastructure will be curtailed without well secured end-user computers and servers' machines -that allows academia and other university staff to access and utilize fully available ICT-based services and resources.

Taking advantage of the government decision on computer importation ban lifting and tax waving [2], UDSM has installed more than 3,000 computers at her main campus. Computers of different brands include Dell, Mac, Sun, Compaq, HP, and Siemens [1, 7, 12]. The table below delineates the trend of ICT equipments growth and its distribution within UDSM main campus.

Table 1: Trend of ICT facilities growth (Computers). Source: UDSM ICT policy, Master plan & UDSM website [1, 7, 12]

Year	Average Number of Computers	Location and Usage Description
1990	17	Mostly located at administration building, deans offices, and head of departments. Very few were located in faculties computer labs, and main library
1995	200	Nearly all administration building offices, dean's offices, head of departments, and academia offices. Faculties labs, few in departmental labs, and main Library
2002	2400	Nearly all administration building offices, dean's offices, head of departments and sections, and academia offices. Faculties' labs, departmental labs, and main Library. PAR's at student's hall of residence: hall 1, 5, 7 and Mabibo hostel each with at least twenty computers and one printer.
2007	3,200	More computers deployment were in offices and departmental new Labs *(AVU-LC, computer science department etc)*

Apart from the progress made, protection of these ICT facilities was affected by a number of issues including lack of enforcing security measures, maintenance culture, and ICT facilities failures. As a result

confidentiality, integrity and availability of sensitive information assets stored in these computers/ servers was jeopardised.

3.3 Bandwidth and Utilisation Status

UDSM was the first HEI in Tanzania to have dial-up connection (from London) that was purely used for sending and receiving emails once a day. The service turned out to be not only a burden to the university as a result of higher telephone connection charges but also the limited number of ICT services offered to the community [7]. As an alternative to that, UDSM gradually managed to upgrade her bandwidth from different providers as delineated in Tables 2 below.

However, running cost remains a challenge, for instance UDSM used to pay monthly subscription fee amounting to 9,000 US$ for 1/2Mbps from TTCL. Currently UDSM is paying around 11,000 US$ (subsidised rate) for 1.5/7.5Mbps from AVU [1]. Following that -to maximize bandwidth utilization, UDSM employed a lop-sided link bandwidth strategy "thin up/fat down" as less bandwidth is required to send data to the Internet and more to receive large data [15]. The table below summarises bandwidth upgrading trend at UDSM.

Table 2: Trend of bandwidth growth over the period starting from early 1990's to date. Source: UDSM ICT Policy Master plan, UCCICT and PHEA [1, 7, 9, 15]

Year	Bandwidth (Mbps)	Total Bandwidth (Mbps)	Connection Type	ISP	Usage Description
1990/93	< 0.024	< 0.024	Dial-up	Heath net	Only for sending and receiving emails
1993/97	0.256/0.512	0.768	Leased Line	TTCL	Internet /Email, Research, Library and few networked computers,
1998/2000	0.512/1.024	1.536	Leased Line	TTCL	Internet /Email, Research, Library and networked computers,
2001/06	1/2	3	Leased Line	TTCL	Internet /Email, Research, Library, online services, and networked computers
2006 –	1.5/7.5	9	VSAT	AVU	Internet /Email, Research, Library, online services , and networked computers

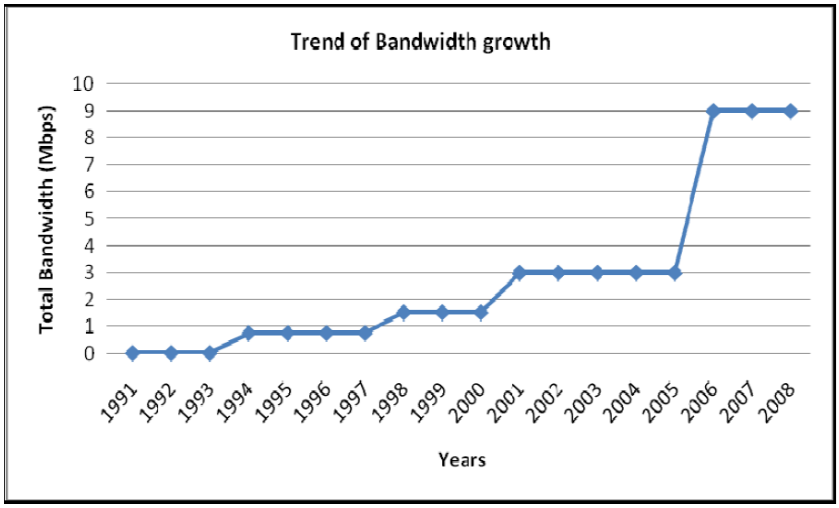


Figure 1: Bandwidth growth starting from 1990's to date

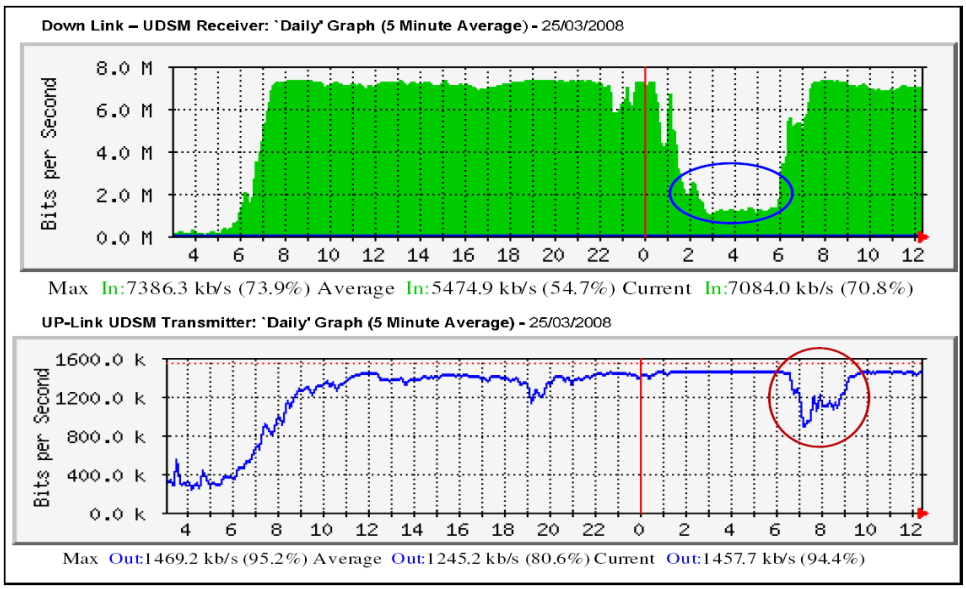


Figure 2: MRTG graphs showing a daily UDSM bandwidth utilisation

Figure 1 shows the bandwidth growth trend while figure 2 shows MRTG daily bandwidth monitoring utilisation graph with down-link of 7.5Mbps and up-link of 1.5Mbps which is over 73% and 95% respectively saturated[3]. UDSM being connected to the outside world via internet was a start for facing new avenues including enhancing teaching, learning, research functions, and library services. However, this process also opens doors to security threats and attacks. A number of measures are taken to minimize these new risks.

3.4 Software's -Operating Systems, Application and Anti-virus

Operating systems (OS) and application programs are the most critical programs for ICT facilities. Malicious code, corruption/destruction of data, and unauthorized change of access rights and privileges are few examples of attacks. To enhance security to these critical assets -awareness, knowledge and technical expertise, and ICT security policies – defining (what, why, how, do's, and don'ts) need to be in place. Patching of operating systems, application programs and use of antivirus solutions are part of security measures that protect ICT assets. As mentioned earlier, the growth in numbers of ICT facilities meant increased software requirements and security demands. Also, more proprietary software's platforms were needed, which demanded UDSM to pay more license fees to vendors while at the same time more bandwidth was required to facilitate downloading and

[3] The circled area in both graphs shows that usage decreases only during the night (from 1 to around 6 hrs). The interpretation tells that most of students do use their laptops to access internet via wireless access points installed across campus while others (including staff family member) who lives in campus do go to Public Access Rooms (PAR) located within the student's hall of resident. Usually at UDSM main campus most of student's departmental computer labs are closed at 20.00hrs with the exception of main library which is closed at 22.00 hrs.

updating of software patches to both servers supporting core services and to end-user computers.

To cut down running cost on software's license fees, UDSM decided to opt for open -access platforms software's – including Linux as OS and Star-office as application programs. This decision was also included in the UDSM ICT policy and master plan [1, 7]. To-date, a fairly larger number of end-user computers and servers are running on open -access platforms [1].

3.5 Information Systems, Online and Library Services

Proper protection procedures against threats that may cause risks to information assets need to be in-place. At UDSM, computerisation and automation process of ICT-based core services and integration of ICT security was not an easy undertaking. As discussed earlier – lack of awareness, knowledge, technical experience and expertise on ICT security were among the major constraints to the process. Thus to ensure that information systems are securely implemented -UDSM had to train her IT staff and was sometimes forced to hire experienced experts / personnel's from abroad [1, 7, 9, 16].

To-date UDSM network infrastructures including existing information systems that are accessible online have fairly high security level. Attackers usually use techniques including cross-site scripting, cookies poisoning & hijacking, content spoofing, denial of service attacks, phishing, man-in-the-middle, or brute-force to exploit vulnerabilities and cause risk/ damage to information assets. Some of the security techniques implemented at UDSM to protect information systems include encryptions, authentication, transport layer security protocols, public key infrastructures – PKI, and virtual private networks. Also automatic backup and disaster recovery solutions were implemented to ensure data availability.

Some of the existing information systems that supports teaching, learning research functions, library and administration services are:

- Teaching/learning: Online systems like Blackboard etc.
- Online Laboratories: iLab – based on real time
- Online Library Services: Online Public Access Catalogue (OPAC), Library Information System (LIBIS), UDSM virtual library, Database for African Theses and Dissertation (DATAD), and Internet search engines and information gateways

- Admission and Examinations: UDSM has developed in-house Academic Registry Information System (ARIS) based on open – access
- Administration: Human Resource Information System (HURIS), and Financial Information System (FIS)
- E-mails and Intranet Services: A number of email services are available.

Apart from success made, still UDSM is facing a number of security challenges that needs special attention.

4 CHALLENGES AND COUNTERMEASURES

The evaluation of computerisation, automation and management of ICT security at UDSM was affected by a number of challenges. These challenges affected much of the fusion and integration process of ICT security with ICT network infrastructure. We categorise the current critical challenges in the following manner: Awareness and capacity building, social-culture, economical, regulatory, technological, power supply, bandwidth and countermeasures.

4.1 Awareness and Capacity Building

Under this category the following were identified as the most critical issues: lack of ICT security awareness and culture among end-users; lack of user knowledge to proper use of ICT facilities including computers – that leads to violation of security procedures; lack of knowledge, practical and technical experiences to IT staff on the higher level implementation and management of both ICT network infrastructures and ICT security.

Others were: lack of technical expertise in defining security requirements and specifications for software's and hardware's before procuring and/or development; inadequate ability to quickly adjust and respond to rapid ICT technological changes – mostly of technological changes occurs in software's development and change of versions; and lack of expertise in maintaining different ICT components/ equipments – notably these requires specialised skills.

4.2 Social-culture

Social-culture behaviour was also seen to be among the challenges in the studied environment. These include: Presence of vandalism on ICT infrastructures and facilities that cause(s) heavy financial loss and service interruption – theft of ICT facilities including network components; and

lack of maintenance culture of ICT facilities among end-users, management and/or decision makers.

4.3 Economical

In this class the following challenges exist: Presence of high experienced IT staff turnover – as a result of high market demand; limited funding that would support proper implementation and management of ICT securities from the institutions and/or government; presence of higher software maintenance and license fees for use of proprietary software's[4]; and presence of higher bandwidth charges[5].

4.4 Regulatory

Regulatory issues were also of concern. Lack of properly defined ICT security policies, procedures and guidelines; and presence of limited support and commitment from the government and/or regulatory bodies on ICT related issues; are some of the challenges that do exist.

4.5 Power Supply

Stable and reliable power supply is a prerequisite needed to smoothly run and operate ICT facilities/ equipments, else survivability of ICT equipments and service availability are jeopardised. At UDSM lack of reliable power supply from the national grid that may cause facilities and systems failure and service interruption, and presence of limited number of un-interrupted power supplies (UPS) to support computers and its facilities are existing challenges.

---

[4] For instance - UDSM pays every year an annual subscription fees for HURIS, FIS and LIBIS amounting to 7,260.00 US$, 26,303.00 US$ and 5,193.51 Euro respectively [7]

[5] "... in Europe and North America a bandwidth that cost 100 US$ a month would cost African universities more that 10,000 US$ a moth..." [15]

4.6 Technology and Bandwidth

ICT is dynamic, this creating a lot of challenges to the ICT security paradigm. These challenges include: presence of malicious codes and alike, including attackers / hackers – exploits network vulnerabilities and cause heavy damages/losses to valuable information assets; limited bandwidth ¬that affects core services availability; and Systems complexity – as most of the systems became more complex, they become more demanding and require high skills to use. Others are presence of fake ICT related equipments in the market and/or vendors – leading to systems failures, service interruption and financial losses; and rapid ICT technological changes.

4.7 Countermeasures to Critical Challenges

To address cited critical challenges, UDSM implemented various countermeasures to mitigate risks and associated damages. These countermeasures are presented and discussed in this section.

4.7.1 Awareness and Capacity Building

As presented, awareness and capacity building is the cross cutting factor that influenced ICT security at UDSM. The programmes for awareness creation are in place. For instance during the start of new academic year all new admitted students are oriented with “don’ts” and “do’s” on use of ICT facilities at UDSM including security issues. However the challenge remains as the students have different backgrounds on ICT knowledge. Also seminars and short-courses related to ICT awareness and use at UDSM are conducted on regular basis to staff at all levels [1, 9].

To build capacity for IT staff, UDSM trained a number of IT staff within and outside the country including professional training[6] and at academic level[7]. Best-practice-study-tours and in¬house were also introduced [1, 9]. For the past five years, ICT security courses have been integrated to some diploma, degree, postgraduates and masters programmes. Also computer literacy courses are mandatory to every degree program at UDSM. Some of the programmes at UDSM that have included ICT security in their curricular continuum are listed below [5, 9, 13]:

- Faculty of Informatics and Virtual Education (FIVE): Certificate and Diploma in Computer science(1/2 yrs); BSc in and BSc with Computer Science (3 yrs); BSc in Electronics and Communication (3 yrs); MSc in Computer Science (2 years); MSc. in Electronic Science and Communication (2 yrs); MSc in Health Informatics (2 yrs); and PhD (3/4 yrs)
- Faculty of Science: Postgraduate Diploma in Scientific Computing (1 yr);
- Faculty of Electrical and Computer Systems Engineering (ECSE): BSc. in Computer Eng. and IT (4 yrs); BSc. in Telecommunications Engineering (4 yrs); Postgraduate Diploma in Electronic and IT (1 yr); MSc in Electronic Engineering and IT (2 yrs); and PhD (4 yrs)
- Faculty of Commerce and Management: Postgraduate Diploma in ICT Policy and Regulation; and Masters in ICT Policy and Regulation (2 yrs)
- University Computing Centre (UCC): Certificate and Diploma in Computing and IT (1/2 yrs). Professional courses: CISCO

[6] For instance -in July 2004, four IT staffs were trained in India at CCNP level; December 2005, three IT staffs were trained in MySQL database administration in Singapore.

[7] For instance -in 2000 seven IT staffs were trained to licentiate and four to PhD level in Sweden.

Internetworking (CCNA, CCNP); Microsoft (MCSA, MCSE etc); IT Essentials; Programming; Oracle (OCDBA, OCP etc) and professional certification.

In addition, the completions of four PhD's (2000 – 2007) in the area of ICT security, their findings and developed model/frameworks have contributed to improvements of ICT security status, not only at UDSM but also in the country [3, 8, 10, 11].

As of today, UDSM has good experience, technical capacity, and expertise in implementing and managing ICT security in network infrastructures. These achievements are due to rising awareness among UDSM community members, recruiting some graduates from the above listed programmes, involvement of the mentioned PhD's graduates and large support from the UDSM management and community.

4.7.2 Social-culture issues

UDSM introduced policies on physical security for protecting her ICT network infrastructures and its facilities. Checkpoints were introduced at the main gates and main buildings entrances where people declare their ICT-related belongings. The numbers of incidents have reasonably gone down. In addition, culture on adhering to maintenance schedules of ICT facilities/ equipments among decision makers is fairly high.

4.7.3 Economical issues

IT staff turnover and retention, UDSM has relatively increased IT staff salaries, as a result staff turnover ratio has significantly gone down to 4.7%. However, the challenge remains as the market salaries are still at high - which could impact staff retention strategies.

To reduce huge amount paid to vendors as maintenance and licenses fees for use of proprietary software's; UDSM has set a policy to migrate from proprietary to open-access software's. To date most of end-user computers (particularly in computer labs) are running on Linux and star-office programs. At the moment (2008) 98% of all servers at UDSM are running on open-access platforms. UDSM is now developing her own information system using open-access platforms; a good example is the developed academic registration information systems (ARIS).

Internet bandwidth charge still remains high despite efforts made by various existing initiatives. To-date UDSM is paying more than 11,000.00 US$ at subsidised rate a month for a total bandwidth of 9Mbps.

4.7.4 Policies and Regulatory

The first UDSM ICT policy and ICT master plan was developed in 1995. Likewise national ICT policy was developed in 2003. The existence of these documents has contributed to the improved of ICT security at UDSM. However, as ICT is very dynamic, challenges remains on proper translation of policy documents in to actions. Also to avoid ad-hoc, timely updating of policy documents to match with the current changes still needs great attention.

4.7.5 Power Supply issues

To mitigate the risks to stable and reliable power supply UDSM installed single and centralised un¬interrupted power supplies (UPS) in offices, computer labs and server rooms. Also automatic standby power generators were installed to strategic areas like theatre rooms, main library, administration and some faculty/departmental buildings. However, the challenge remains on the sustainability of maintaining and running these generators as they require periodical maintenance ¬fuel and spare parts – that requires funding.

4.7.6 Bandwidth and Technological issues

A rapid technological change has forced ICT-based service users always to be at alarming state. UDSM faced a lot of critical technological challenges as presented in section 4.6. However to mitigate the risk UDSM implemented a number of strictly measures to secure her network infrastructure and critical assets against threats that may exploit vulnerabilities and cause risk to information assets. Implementation of tools (hardware's and software's) and configuration techniques including intrusion detection systems (IDS), firewalls, routers, intelligence switches and virtual LAN (VLAN) as part of measures to secure the network infrastructure is done.

Also to enhance confidentiality, integrity, authenticity, authentication, accountability, and non-repudiation to web-based information systems security techniques including -encryption, authentication, TLS, public key infrastructures – PKI were also implemented. Furthermore, automatic and manual data back-up mechanisms, including disaster recovery solutions are

in place. Monitoring and management of network infrastructure is now automated. Tools like "What's-Up-Gold" are in use. The use of such tools has significantly simplified management of network infrastructures, where from one central location IT staffs are able to monitor the entire network depending on the configuration.

For control of viruses and malicious codes, UDSM has implemented a university wide Antivirus solution "escan corporate solution" which is centrally accessed. In addition, all up-to-date patches are also centrally kept and accessed -this technique facilitates easy access and timely availability to networked end-users computers, hence international bandwidth serving.

Addressing the bandwidth problem, despite of efforts made by UDSM to manage the little bandwidth it has, still challenge remains as ICT-based core services are affected. Some of counter¬measures that are in place include:

- Use of bandwidth manager: Internet bandwidth is now allocated per network segments (sub¬networks), this technique also facilitates retention of any un-usual generated traffic not to affect the rest of the network
- Traffic divergence: All UDSM local traffic generated from accessing of local emails and websites are routed through TIX[8]
- Patches and Updates: patches and updates files for operating systems, application programs, and ant-viruses are kept and accessed locally at the central servers. Authorised users are allowed to update their computer patches from the central servers (locally).

[8] Tanzania Internet Exchange (TIX) is a national internet exchange centre that keeps local traffic (local emails and websites) local. This leave international bandwidth to be used for other services.

- Blocking of international online web-based emails: yahoo, hotmail and alike are blocked during working hours where bandwidth is mostly needed for supporting core services. After working hours these web-based emails are allowed when much of the bandwidth is un-used.

Despite of all efforts made to manage sufficiently the little bandwidth UDSM has, still more bandwidth[9] is needed (approximately six times of the current bandwidth) to support more than 3,000 networked computers together with automated ICT-based core services.

5 DISCUSSION AND LESSONS LEARNT

The overall goal for implementing, fusion and managing ICT security into network infrastructures is to secure critical information assets. However, from the analyses we have seen that there are a number of current critical challenges that affect proper and secure implementation, fusion and management of ICT security paradigm. Furthermore, we have seen how UDSM critically addresses these challenges, though fairly few still remain. Based on the analyses and discussions on current challenges at UDSM – we sift out the following as lessons learnt:

- Higher bandwidth charges in Africa, undermines automation process of ICT-based core services and quality service delivery. Due to the limited bandwidth most HEI has, proper measures and policies on its utilisation are required. Bandwidth management techniques such as these implemented at UDSM (discussed in section 4.7.6) may be applied.
- Automation of network infrastructure management at UDSM enabled IT staff to easily manage and monitor the entire network from a single

[9] "...An institution with an average of 3,000 networked computers with automated ICT-based core services requires at least 66Mbps..." [15].

location. As discussed in section 4.7.6 – this has led to time and cost serving, and improved efficiency in managing ICT Security.

- From the discussion presented in section 4.7.1, we have seen that in order to create awareness and building internal capacity, special initiatives are needed. UDSM integrated computers and ICT security related courses/programmes at different levels within university academic curricular. These efforts facilitated also the generation of more IT security specialists.
- The study revealed that defining ICT security requirement specifications for hardware's and/or software's products remains a challenge. Proper attention should be given on developing measures to build internal capacity in the area.
- The discussion (section 3.4 and 4.7.6) shows that so far UDSM has successful implemented security mechanisms. The challenge remains as technology keeps changing – new threats and risk are always at alarming states.
- Dependence on proprietary software undermines development of HEI as much financial resources are required for payment of maintenance and annual subscription fees[10]. Therefore, for the survival of HEI, the migration strategies to open-access software are necessary.
- From the discussion (section 3.5) we have seen that UDSM managed to develop in-house ARIS system using open-access software. Thus HEI(s) could build their internal capacity to develop software in-house.
- Fusion of both ICT security policies to networks, email acceptable use etc, are necessary for enhancing information security at HEI. Top

[10] UDSM is paying every year an annual subscription fees for HURIS, FIS and LIBIS amounting to 7,260.00 US$, 26,303.00 US$ and 5,193.51 Euro respectively.

management support is highly needed for successful implementation and enforcement of these policies.

- ICT-based services should be available when needed. From the discussion in section 4.5, we have seen that UDSM managed to install automated standby power generators in strategic areas and most of end-users computers are connected on UPS(s) -single and centralised ones. Thus HEI(s) in Africa should invest in emergency power supplies.
- Selling of fake ICT equipments (especially in Africa) is emerging which leads to systems failure. The study revealed that -the problem is very challenging and needs to be handled collectively.
- IT staff turnover ratio at UDSM has significantly gone down to 4.7% by July 2004. Good salary and a conducive working environment are contributing factors to the success. HEI(s) in Africa should develop IT staff retention strategies.

In order to be able to visualise the relationship between specific elements in our analysis and discussion-it would be fruitful to identify in particular what actions the university itself can be and is in control of and what actions and items the university cannot control by itself but only influence within a longer time frame. Such an analysis is provided.

The proposed framework is based on internal and external elements. The internal elements are these activities that UDSM has control of itself; while the external ones are these that UDSM has no control of (influencing factors from the environment). The input elements are processed and the output is called ICT security management. Since there is no single solution for ICT security management, hence the input -output process is repetitive.

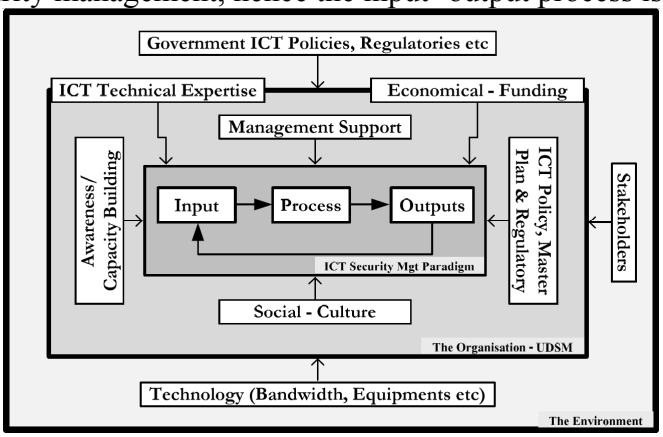


Figure 3: Proposed ICT Security Management Framework based on UDSM experience

6 CONCLUSION AND RECOMMENDATIONS

As information and communication technology is considered to be a major driving force of globalised and knowledge based society in the modern world – proper fusion and integration of ICT security to network infrastructures should be given higher attention. In the paper, the process of computerisation, automation and management of ICT security from early 1990 were presented. In the analysis -challenges were categorised into: Awareness and capacity building, Social-culture, Economical, Regulatory and Policies, Power supplies, and Technology and Bandwidth. Counter¬measures were discussed at length and lessons learnt were presented. In addition, the framework based on UDSM experience in ICT security management was developed and presented.

Generally we have seen that for better ICT service delivery -ICT security is highly needed for protection of critical information assets. Therefore, it is recommended that special attention should be given to the addressed issues that are still affecting ICT security paradigm. Furthermore, we believe that the presented UDSM experience in the area could also be adopted by other universities in the developing world.

7 REFERENCES

[1] UDSM-ICTP, University of Dar es Salaam, ICT Policy, May 2006

[2] TZ-ICT, Tanzania National ICT Policy, March 2003. Available at http://www.tanzania.go.tz/
[Accessed on 25th March, 2008]

[3] Bakari, Jabiri, "A Holistic Approach for Managing ICT Security in Non-Commercial Organisations: Case Study in a Developing Country", PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, 2007. ISBN: 91-7155-383-8

[4] ITU, "Improving IP connectivity in the least developing countries" (2002)

[5] UDSM-DUS, Directorate of undergraduate studies -UDSM "Undergraduate Programmes and Admission procedures" (2007)

[6] TCRA, Tanzania Communications Regulatory Authority website: http://www.tcra.go.tz
[Accessed on 25th March, 2008]

[7] UDSM-ICTM, University of Dar es Salaam, ICT Master Plan (2008 – 2012), September 2007

[8] Tarimo, Charles, "ICT Security Checklist for Developing Countries: A Social-Technical Approach", PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, 2006. ISBN: 91-7155-340-1

[9] UCC-ICT, University of Dar es Salaam-Computing Centre website: http://www.ucc.co.tz, [Accessed on 27th March, 2008]

[10] Casmir, Respickius, "A Dynamic and Adaptive Information Security Awareness (DAISA) Approach", PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, 2005. ISBN: 91-7155-154-9

[11] Chaula, Job, "A Social-Technical Analysis of Information Systems Security Assurance", PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, 2006. ISBN: 91-7155-339-8

[12] UDSM, University of Dar es Salaam website: http://www.udsm.ac.tz, [Accessed on 25th March, 2008]

[13] UDSM-DPS, Directorate of Postgraduate studies -UDSM "Postgraduate Programmes and Admission procedures" (2008/09)

[14] Webometrics Ranking, http://www.studysa.co.za/contentpage.aspx?pageid=4150 [Accessed on 25th March, 2008]

[15] PHEA, http://www.foundation-partnership.org/pubs/pdf/more_bandwidth.pdf

[16] UDSM-Lib, University of Dar es salaam, Library: http://library.udsm.ac.tz

[17] Luhanga, M., and Mashalla, J., "Reforms and innovations in higher education: A reflection on the initiatives and lessons at the University of Dar es Salaam in Tanzania". A paper prepared for a Nuffic Conference on Higher Education, (2005)