TOWARDS MANAGING ICT SECURITY IN NON-COMMERCIAL ORGANISATIONS IN DEVELOPING COUNTRIES

Jabiri Kuwe Bakari[1], Louise Yngström[2], Christer Magnusson[3], Job Asheri Chaula[4]

Department of Computer and System Sciences
Stockholm University/Royal Institute of Technology

Forum 100, SE-164 40 Kista, Sweden
Tel: +46 (0)8 674 72 37
Fax: +46 (0)8 703 90 25
E-mails: {si-jba[1], louise[2], cmagnus[3], si-jac[4]}@dsv.su.se

ABSTRACT

The use of ICT in developed countries has changed economies and the way businesses run. The use and development of ICT capabilities however, faces a wide range of constraints and challenges in the developing countries. These constraints include the country's historical background, culture, poor or lack of infrastructure, education, social, legal status, political, attitude and preparedness towards use of ICT. Others are absence of ICT policy, implementation procedures, general lack of appropriate knowledge on ICT (among suppliers, managers, planners, and users), few trained or skilled ICT personnel as well as financial constraints. Both commercial and non-commercial organisations are busy with "Computerisation" paying very little attention to how to use these ICT, security of critical ICT assets, and consequently their effect on the organisation's objectives. Most of the present ICT security control measures are only on an ad hoc basis.

This paper gives an overview of ICT security problems in developing countries and attempts to address the challenges involved in managing ICT security, paying more attention to non-commercial organisations. The developing countries would not intend to go through the 30 years most developed countries have taken, because, after all, developing countries are already a part of the developed world system (the Internet) and in fact, the technology in use in this part of the world is state of the art technology. However, the problems and challenges being faced now are neither the same ones the developed countries are currently facing nor those of the last 30 years. This being the case, ICT weakness in the developing world has the potential of being the weakest link in the Internet. A Systemic-holistic approach to this multi-disciplinary problem is proposed. Business Requirements on Information Technology Security (BRITS) framework have been identified for deployment in five non-commercial organisations during which the workable guidelines/criteria for managing the ICT security in the developing world will be formulated. BRITS is a systemic-holistic framework, combining finance, risk transfer, IT and security in a coherent system.

KEY WORDS

ICT Security management, Non-commercial organisations, developing world, Systemic holistic approach, BRITS.

TOWARDS MANAGING ICT SECURITY IN NON-COMMERCIAL ORGANISATIONS IN DEVELOPING COUNTRIES

1 INTRODUCTION

The use of Information and Communication Technologies (ICT) in Developed Countries has led to tremendous changes in the economy and even the way people live. However in the developing world the use and development of ICT capabilities is still limited and faces a wide range of constraints and challenges [Wanyembi et al., 2000], [Moyo, 1996] and [Valantin 1996]. These constraints include those associated with the historical background and culture, such as poor (or lack of) infrastructure and education, poor social, legal and political attitude and preparedness towards use of ICT, absence of ICT policy or its implementation procedures, general lack of appropriate knowledge of ICT (among suppliers, managers, planners and users), few trained or skilled ICT personnel and severe financial constraints. Such problems lead to many challenges, especially when it comes to implementation in particular for management, control and maintenance. [Wanyembi et al., 2000] points out that the rapid diffusion of ICT in many organisations in developing countries is a new and growing phenomenon, which presents serious challenges. He further asserts that, while vast amounts of hardware and software are acquired in increasing quantities, users' expectations of improved services are not fulfilled, partly due to the low quality of management and maintenance of ICT. [Moyo, 1996] and [Valantin 1996] point to the infrastructure, especially communication infrastructure, bandwidth size and power interruption as the source of the problems in the application of ICT in the developing world. People's literacy levels, language ability and cultural background, as well as their age and attitude towards modern technologies are also inhibiting factors in appreciating the use of ICT. [Massingue, 2003] argues that the knowledge necessary for effective use and exploitation is not being transferred at the same speed as the technology itself.

Of particular interest is the observation that organisations in this part of the world are investing much in the design, procurement and to some extent deployment of computers and building Local Area Networks (LANs), referred to as "Computerisation". Deployment of ICT is not part and parcel of organisational reform or business re-engineering. Very little or no attention at all is paid to how to use these ICT. More serious is the security of critical ICT assets, and consequently their effect on the organisation's objectives. Most of the present ICT security control measures are only on an ad hoc basis and users have expressed frustration due to unfulfilled expectations of the performance of the new technology [Wanyembi et al., 2000]. In order to address these challenges, organisations in developing countries are attempting to use existing solutions (standards, frameworks, models, etc.) that promise to solve these problems, which are similar to those found in the developed world. However, the study of many of these available solutions reveals that most of them have themselves inherent limitations and are largely costly, impractical, consume a lot of time to implement and do not address the situation-specific problems that are unique to organisations in the developing world [Wanyembi et al., 2000]. Certainly there are organisations which have deployed some of these solutions, but due to the users' limited knowledge of proper usage and management, the issue is left to suppliers who often take the advantage of supplying whatever they have in stock.

The purpose of this research paper is to address the challenges involved in managing ICT security in developing countries' environment, taking Tanzania as a case study. It attempts to build workable guidelines to be used as criteria for managing ICT security based on Business Requirements on Information Technology Security (BRITS) framework. The problem that is being addressed is multi-disciplinary in nature. This means it involves various disciplines such as culture, legal, policy and technology and calls for the framework or model to be based on a systemic-holistic approach as suggested by [Yngström, 1996], with security by consensus (SBC) approach as

suggested by [Kowalski, 1994]. These two concepts facilitate interdisciplinary considerations. BRITS is a Systemic-Holistic framework, combining finance, risk transfer, IT and security in a coherent system. BRITS framework has been accepted and implemented in banking, broking, logistics, e-commerce and insurance companies in Sweden in the last 8 years and has yielded successful results. BRITS framework has been considered because of its holistic nature and ability to assist ICT-dependent organisations in protecting losses due to ICT risks. The research explores to see if the holistic perspective of BRITS makes it possible to utilise it in non-commercial organisations in the developing world.

The paper starts by giving an overview of ICT security problems in the developing world and the comparisons of ICT use and capabilities between the developed and developing world. Developing countries are in general countries that have not achieved a significant degree of industrialisation relative to their populations, and which have a low standard of living [Wikipedia, 2004]. Throughout this paper, the term developing world is used interchangeably with the term developing countries. The discussion focuses on the challenges involved in managing ICT security in non-commercial organisations by taking Tanzania as a typical example of a developing country. Developing countries have no intention of going through the 30 years most developed countries have taken since, after all, they are already part of the developed world system (the Internet) and in fact they are also forced to use the current technology. However, the problems and challenges the developing countries are facing now are neither the same ones the developed countries are currently facing, nor those of the last 30 years. The intention is not to re-do what the developed world has gone through, but use the available solutions, paying more attention to the environment of developing countries.

The proposed BRITS framework will be deployed in five non-commercial organisations in Tanzania, during which workable guidelines/criteria for managing the ICT security in the developing world will be proposed. In the last section of this paper, five steps explaining our research approach in deploying BRITS are presented. It is expected that during the deployment of the framework we shall be able to (a) formulate the workable guidelines (set of criteria) needed to successfully manage ICT security in developing countries, and (b) validate the suitability of the BRITS framework for application to non-commercial organisations.

2 COMPARISON OF ICT USE AND SECURITY TREND

Accessibility of various communication devices such as TV, Radio, Telephone and Personal Computers is far greater in developed countries than developing countries with developing countries taking the lowest share as seen in table 1.

Table 1: Access to various ICT

Indicators	**U.K.**	**Sweden**	**South Korea**	**Tanzania**	**Mozambique**	**Nigeria**
Radio per 1000 people	1,436	932	1,033	279	40	223
Television per 1000 people	645	531	346	21	5	66
Telephone per 1000 people	557	674	433	4	4	4
Mobile phones per 1000 people	253	464	302	1	0	0
Personal Computers per 1000	263	361.4	156.8	1.6	1.6	5.7
Internet host per 10,000 people	321.39	670.83	60.03	0.06	0.09	0.01
Scientists and Engineers in R & D per million people 1987-1997	2,448	3,826	2,193	..	..	15

Source: World Development Report 2000/2001, ICT PP 310-311[World Bank, 2001]

There is no doubt from the figures in table 1 that there is a big gap in terms of ICT capacity and usage between the developed and developing world. This is due to poor infrastructure, financial

capabilities, low level of education and sometimes ignorance. From the literature review and our experience, most developing countries are beginning to deploy ICT. Attention is on deployment rather than the use and control; yet security problems are growing. Studies by [Klijfhout, 1996], [Massingue, 2003], [Casmir & Yngström 2003] and [Bhattarakosol, 2003] talk about challenges involved in the implementation of ICT in this part of the world. [Klijfhout, 1996] argues that the introduction of ICT in developing countries is heavily dependent on external initiators, which in turn leads to processes which hinder the development of a local knowledge base, and which propagates dependence on external experts. By using Swaziland as a case study, he also looked at the role of culture and the nature of technology in the process of transfer. [Massingue, 2003] argues that the ICT environment in SADC (Southern African Development Community) countries, with the exception of South African and Mauritius, is characterised by weak infrastructure, a multiplicity of equipment and software types and a very limited research and education base to strengthen professional approaches to management. These situations suggest the possibility of high ICT risks and consequently high costs in dealing with the problem. It is also worth noting that the developed countries are making some effort at enforcing the use of standards such as ISO 17799 in the public and private sectors, on the management side, and on the production line common criteria (CC). There are various initiatives being given priority, for example as far as legal is concerned, such as the EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [EC46, 1995].

The security of information systems is a serious issue because computer abuse is increasing (see figure 1) not only in the developing world but also worldwide.

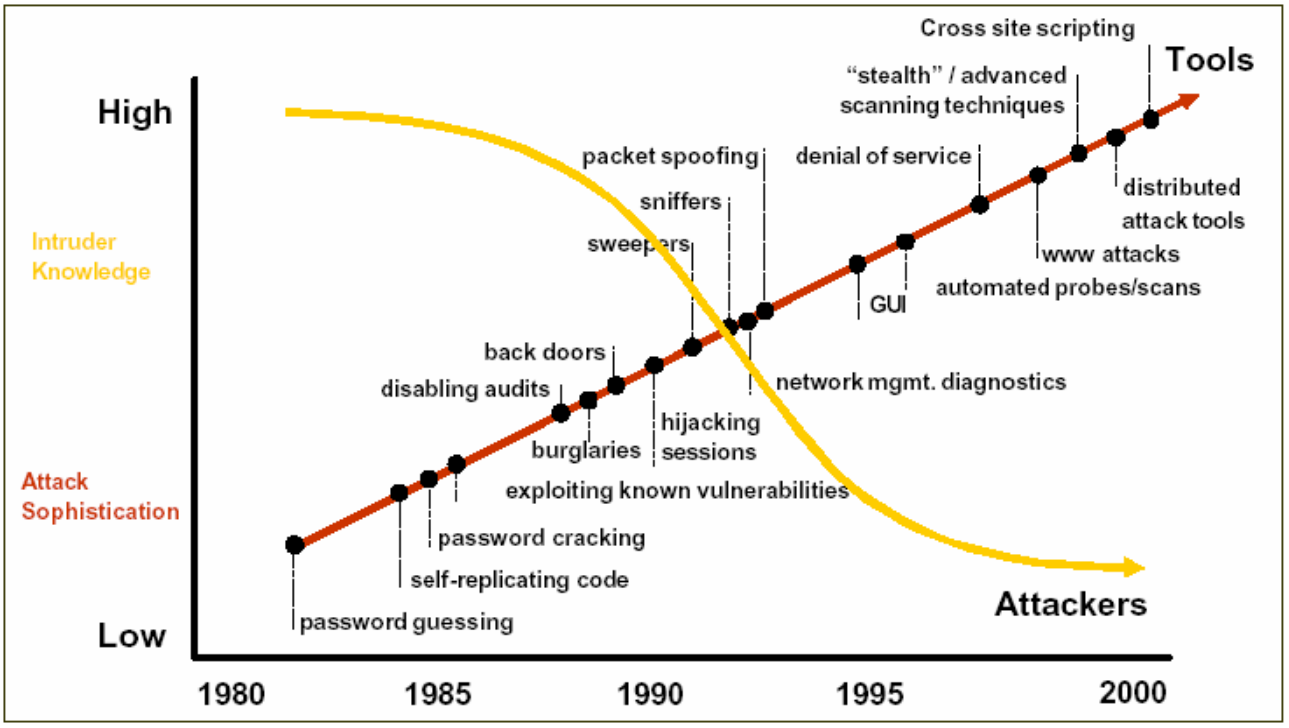

Figure 1: Attack sophistication Vs Intruder knowledge, source: [Cert, 2003]

ICT security-related cases are not going away and are expected to increase further as the computer literacy rate improves. Predictably, it can be assumed that, for every case detected, there are more cases unreported and even more undetected, given the absence of proper ICT security management. The figure shows that as the attack sophistication increases, the knowledge required by attackers to carry out the attack is decreasing which means more security problems.

3 ICT SECURITY IN TANZANIA

The significant achievement of ICT in Tanzania can be traced from early nineties[1] after various adjustments in policy, regulatory and commercial facets, both macroeconomic and within ICT's converging sectors [TzICT, 2003]. Since then, Tanzania has experienced dramatic changes in the use of ICT, coupled with limited knowledge, use of different software and hardware imported from different places of the world, poor communication and power infrastructure and poor control and maintenance of the ICT in general. Significant developments can be traced from 1994 when the first TV station started broadcasting, with the establishment of mobile phone companies in 1995, and when Tanzania was connected to the Internet for the first time in 1996 [MEA, 2001; Casmir & Yngström 2003]. Table 2 indicates key ICT statistics indicators in Tanzania.

Table 2: Key ICT statistics indicators in Tanzania

Indicators	**1961**	**1993**	**2002**
Population (in Millions)	12.3	26.7	33.6
Fixed line exchange capacity	11,300	125,703	234,640
Mobile operators		1	4
Mobile subscribers		1,500	700,000
Teledensity (lines per 100 people)	0.1	0.32	1.22
Data communications operators			16
Internet service providers		1	23
Internet subscribers (Dial-up accounts and Wireless)		10	14,000
Internet capacity (Total bandwidth Kbits)		64	44,000
Television licences		1	24
Radio broadcast licences	1	2	18
Indicators	**1961**	**1993**	**2002**

Source: Tanzania National ICT Policy [TzICT, 2003]

At the individual level, people are purchasing computers for home use, getting dial-up connections, enrolling in short courses on how to use PCs, etc. On the organisational level, efforts are mainly aimed at purchasing computers, installing various information systems and to some extent training staff on how to use computers. In other words, it is in the initial phase, where people are changing from manual to computerised systems.

The survey conducted in 2001, to find out the status of the ICT in one of the universities in Tanzania, which is typically a large non-commercial organisation[2], showed that the number of computers had increased by more than 800% from 1995 to 2001. The survey indicated that, since 1996, five information systems have been installed with probably the best network infrastructure in the country. Figure 2 shows the percentage of different brands of PCs with the non-brand or clones (67.8%) taking the largest share, and running on top of different operating systems ranging from Disk Operating System (DOS), various versions of windows, various versions of Linux, Macintosh, etc.

[1] Tanzania attained independence in **1961**.

[2] For confidentiality reasons the name of the organisation is not disclosed

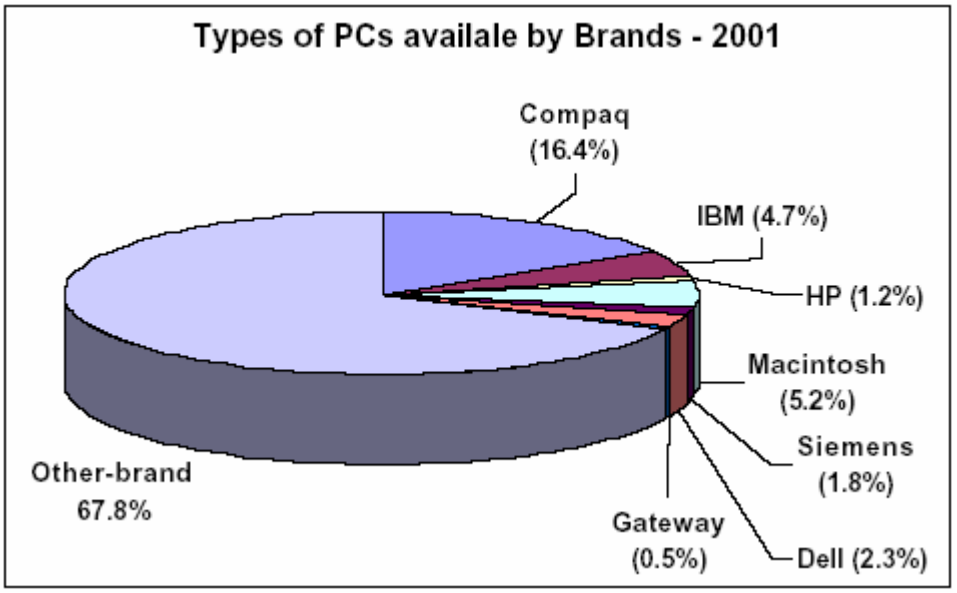

Figure 2: Types of PCs available by brands at the University, source: [Surveyed data by Bakari & Mboma, 2001]

25.1% of these PCs were connected through the UPS or power stabiliser. Although the study indicated that, most of these PCs were bought with UPS or power stabilisers, most of UPS/Stabilisers were malfunctioning due to power fluctuations. Power fluctuation accounted for more than 24.2% of all problems in ICT equipment reported at the university's IT unit. Viruses were found to be the main source of problem and accounted for more than 51% of reported incidences. The differences in brands/capabilities, operating systems and application packages add to the complications involved in attempting to solve for example a worm or virus outbreak, causing business interruption and increase in service unavailability time. Furthermore, the power fluctuations have been a cause of hardware destruction, denial of service, data corruption and in some cases losses, in particular when it happens in the middle of data/information transitions.

At the national level, the national ICT policy has been put in place and various public and private sectors are now in the process of computerisation. However, there are islands of information systems that are not integrated, partly due to poor or completely absent infrastructure and partly due to the absence of policies and/or directives. There are very few kilometres of fibre optic in the city centres with domination of wireless technology. Absence of usage policy in most organisations allows users to make their own decisions on how to handle and use the organisation's ICT assets. These observations and others made by [Mbwette & Mboma, 2000] show how fast the dependence on ICT is growing on a daily basis and hence exposure to ICT risks.

Several trends in ICT are identified, including the rapid diffusion and dependence on ICT in many organisations, which have brought challenges and raised doubt as to the sustainability of the application of ICT in fulfilling organisations' objectives. For example: it is now becoming common to walk into an office for a particular service just to be told that the service is not available because the system is down due to a virus; there are no services available at the bank for some hours because there is some problems in the system (no explanation given); the salary will be delayed because there are some problems in the system, etc. The number of reported incidents of breach of security where huge sums of money are said to have been disappeared or stolen through computer fraud is increasing [Casmir & Yngström 2003]. An example of this can be found in the East African Fraud report survey [KPMG, 2002] where 82% of the respondents considered their computer and information systems to be a potential security risk. As main reasons for the increase in fraud, the respondents in the report also pointed out: lack of adequate penalties and enforcement (53%); inefficiencies of the justice system (61%); sophisticated criminals (72%); furthermore, 64% of the respondents indicated that suppliers are the source of the largest financial losses.

These trends show deficiencies in ICT legal framework, harmonised security and systems standards, lack of appropriate knowledge (users, planners, managers and among suppliers) and general stakeholder security awareness. Observations made in various papers in the introduction have indicated some degree of vulnerability of the implemented systems and some have gone further by giving highlights of the security problems in general. However, they did not indicate what steps are to be taken apart from general ICT management, except the last one by [Casmir, 2003] which is attempting to address the problem from the educational point of view.

4 MANAGING ICT SECURITY IN NON-COMMERCIAL ORGANISATIONS

ICT security management is a combination of several aspects involving policies, standards, guidelines, codes-of-practice, technology, human issues, legal and ethical issues [Eloff & Eloff, 2003]. A comprehensive Information Security Programme contains a proper balance between people, processes and technology to effectively manage risks with minimal impact on the organisation's operations. According to [Bishop, 2003], human beings are the weakest link in the security mechanisms of any system. Human issues may be divided into (a) organisational problems which are lack of resources, lack of trained people and the tendency to consider security issues as secondary ones; (b) people problems grouped into insiders and outsiders. ISO 17799 gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation. However, according to [ISO/IECFAQ 2002], ISO/IEC 17799 does not provide detailed conformity specifications necessary for an organisational information security management program. It does not provide enough information to support an in-depth organisational information security review [ISO/IECFAQ 2002].

While in commercial organisations the main objective is to hedge shareholder value, in non-commercial organisations the main objective is to meet the organisation's missions such as business continuity, deliver quality services, minimise business interruption, eliminate fraud and corruption, minimise loss of property, protect copyright, ensure privacy, ensure confidentiality and minimise consequential liabilities, protect organisation's reputation, etc. The ability of any organisation to achieve its mission and meet its business objectives is directly linked to the state of its computing infrastructure. Although in non-commercial organisations the objective is not to a make profit, risks associated with ICT use do have financial implications too. Therefore, in order to ensure that, the non-commercial organisations meet their objectives, there must be an insurance structure which encompasses insurance policies such as ICT security policies, standards, guidelines, codes-of-practices, technologies, legal and ethical issues to counter the risks associated with ICT.

When a commercial organisation makes a loss, one can make decisions on business grounds such as closing the company, etc. However, one cannot close the non-commercial organisation like a public university or a government ministry for the loss associated with the ICT risks. One of the measures one can take is to estimate the loss on the one hand, which in most cases might be associated with the cost of reactivating the affected services. On the other hand, one can estimate the loss by also associating it with the cost of putting the service right so that that particular problem does not happen again. Finally, and which is more challenging, is working out the estimates associated with those who are affected by the absence of the system/system malfunction (one may call this a social value which in most cases tend to be subjective).

The value of the research at hand is to anticipate such consequences and put in place some measures. The focus of this research is on non-commercial organisations, i.e. organisations that are not profit making but have non-financial objectives and goals to achieve. Such organisations include government institutions like public universities, public healthcare, etc. Many of these organisations have become increasingly dependent on highly complex and heterogeneous ICT-platforms, and hence more exposed to ICT related risks [Magnusson, 1999]. If these risks are not taken care of, the objectives of these organisations will be affected negatively.

4.1 BRITS framework

In the BRITS framework, the need for financial insurance and technical countermeasures against ICT risk depends entirely on the effect these risks may have on the value of the organisation [Christer, 1999]. BRITS use the Discounted Cash Flow (DCF) formula to estimate the loss exposures. The idea behind BRITS is that if an organisation greatly depends on ICT for its financial value then the insurance structure is used to secure against the ICT risks, and thereby secure shareholders' value. The insurance structure (captive structure) is used to provide the company's business services/product with hedge policies (insurance) against financial consequences of ICT risks. Thereafter depending on the cover required, a security policy is produced for the ICT platforms that are responsible for business services. BRITS framework uses the computerised tool called "Estimated Maximum information technology Loss" (EMitL) to develop security policies. This database makes it possible to estimate the costs for the loss exposure inherent in a business service/product in a better way and thereby be incorporated in the product's price [Magnusson, 1999].

5 RESEARCH APPROACH

Based on the exploration made in the paper, BRITS framework has been proposed for implementation in five non-commercial organisations during which workable guidelines/criteria based on the BRITS framework will be formulated along with the validation of the framework. Figure 3 presents a complete design of our research approach.

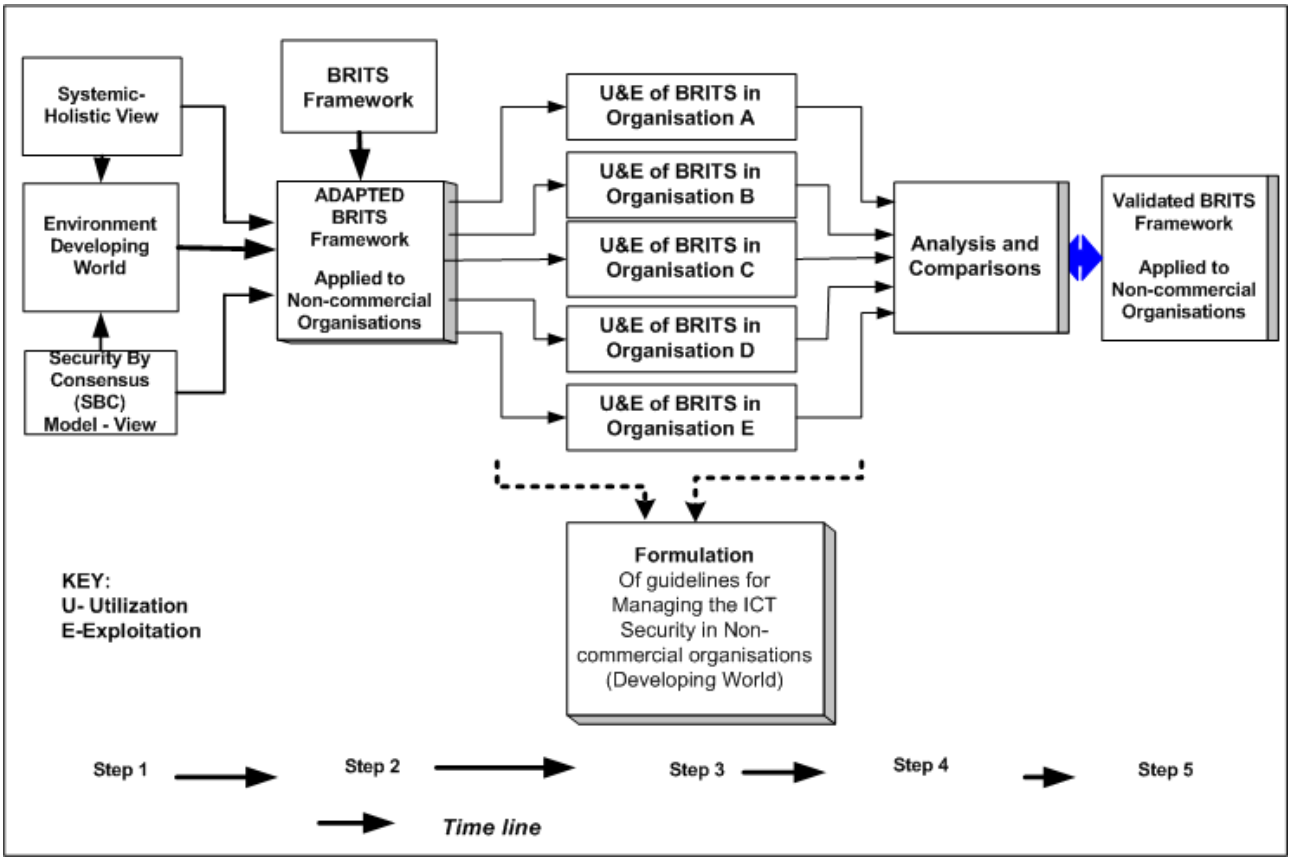

Figure 3: Steps summarising how the guidelines for managing ICT in the developing world is formulated, along with the validation of BRITS framework

Step 1

The work starts by focusing attention on the developing world environment from systemic holistic and security by consensus (SBC) points of view. The content of the Systemic Holistic

Module is based on General System Theory, Cybernetics and General Living Systems Theory. By making use of these theories, we are able to view the whole system as well as its details. These theories about systems offer checklists and rules-of-thumb, by among other things, facilitating interdisciplinary considerations [Yngstrom, 1996]. [Kowalski, 1994] suggests that the ICT security can be modelled as hierarchy of social and technical security measures. He suggests the use of the SBC model when attempting to model both the static and dynamic characteristics of ICT security. The model divides the security into social and technical categories which are further divided into subclasses **social** (Ethical-cultural, Legal-contractual, Administrative-managerial-Policy, and Operational-procedural) and **Technical** (Mechanical-electronic and Information-Data).

Systemic-holistic view and SBC models are used in this work as tools to focus and analyse the environment in the developing world, in order to have a firm understanding of the issues and challenges involved in managing the ICT security in the developing countries and their environment in particular.

Step 2

The second stage is an attempt to apply the BRITS framework with emphasis on the five selected non-commercial organisations. In the BRITS framework process [Magnusson, 1999, Page 123], the need for insurance and technical countermeasures against ICT risk depends entirely on the effect these risks may have on the organisation's objectives [Magnusson, 1999]. Figure 4 shows how these countermeasures are derived from the organisation's objectives.

(i) Identification of Organisation Objectives

In figure 4 objectives are represented by (**O_1, O_2, O_3, O_4 … O_n**). Organisation's objectives, which will be taken into account, are those that are ICT dependent.

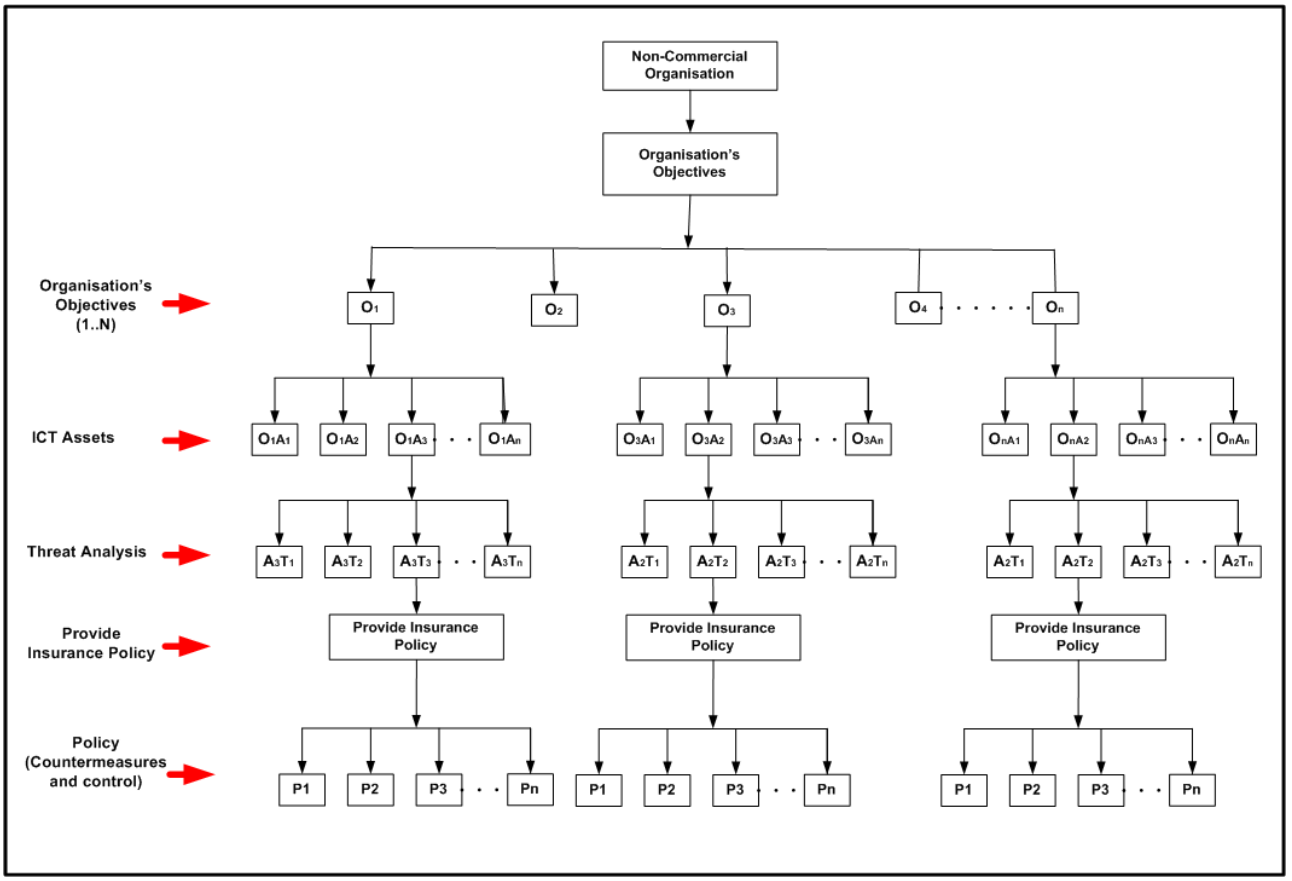

Figure 4: Showing how insurance policies can be derived from the Organisation's Objectives

(ii) Identification of ICT assets that supports the Organisation's objectives

The second stage involves identification of ICT assets that support the organisation's objective/s ($\mathbf{O_xA_x}$) and business's key performance indicators. The ability of an organisation to achieve its mission and its business objectives is directly linked to the state of its information systems. According to [Alberts & Dorofee, 2003], asset is something of value to the enterprise and includes systems, information, software, hardware and people. Systems store, process, and transmit the critical information that drives organisations.

(iii) Analysis of threats to the organisation's ICT assets

The third stage involves threat analysis. For each identified asset, assessment of the threats - ($\mathbf{A_xT_x}$) and their consequences that hinder the organisation from meeting its intended objective $\mathbf{O_x}$ (where **x** identifies the objective and likewise the corresponding threat, and can be from **1** up to **n** threats) - is taking place. If we take the example of business continuity as an objective, then the set of threats can be theft, power fluctuation, virus or Denial Of Service (DOS).

(iv) Ensuring organisation's objectives

The fourth stage involves identification of insurance policy (countermeasures) for each threat. Picking theft in the previous example, the policy ($\mathbf{P_x}$) may include back-up, traceability and recovery, and user policy. The idea behind BRITS is that if an organisation greatly depends on ICT for meeting its objectives/goals then the insurance structure is used to secure against the ICT risks, and thereby secure the organisation's mission. The insurance structure is used to provide the organisation's services with insurance against consequences of ICT risks.

The outcome report (of identified objectives, identified ICT assets, threats and their possible countermeasures) is compared with the current organisation's ICT practices in order to estimate the security awareness in the organisation. The end results is the security benchmarking documented in a survey report that gives an overview of the security awareness and vulnerabilities in the organisation's ICT assets. This report is used to estimate the Expected Maximum Loss (EML) if the identified risks are not mitigated, and thus price the insurance request. The outcome report also can be used to suggest increased security measures. During this stage, the management have to decide if security measures should be increased in the ICT-platform to supports the organisation's core mission. These ICT security measures should be cost effective since there are no other reasons for spending resources on technical measures than a clear link to safeguard the organisation's mission. If accepted by the management the next stage to consider is the underwriting of the insurance request. The security policy and the suggested increased security measures agreed on will then constitute the terms of insurance. As with all insurance policies, there are terms of insurance. In our case, the senior management's decision on the security level for the ICT is the terms of insurance. At least the security awareness achieved in the survey report should be fulfilled in order to have a valid insurance policy [Magnusson, 1999].

The goal here is to design and develop countermeasures tailored to the organisation that will remedy vulnerabilities and deficiencies identified. After this stage, which is mainly analytical, the solutions are still "on the drawing board", the process referred to in Information Security Management Systems (ISMS) [Bjorck, 2001]. The utilisation/exploitation stage takes the conceptual level and makes them work in the organisation. This entails, for example, installation and configuration of technical security mechanisms (e.g. user policy, backup, etc), as well as information security education and training of employees.

Steps 3 & 4

Steps 3 and 4 in figure 3 are meant to illustrate how the deployed BRITS framework performs in the organisation during the Utilisation (**U**) and Exploitation (**E**) for a period of approximately 2

years. After the framework has been put into use, all kinds of feedback will occur as observations. Greater emphasis during this exercise will be on observing the critical issues during the utilisation/exploitation of BRITS framework, such as: what is involved in making such a successful framework in the developed world work in a developing country; where are the difficulties, what guidelines/criteria are required to overcome those difficulties and achieve the required goal? For example, if it turns out that the cost of insuring the risks are found to be very high, how should the proposed countermeasures be given priority, given the environment (for example, poor infrastructure, absence of ICT legal framework etc.). This process is iterative and the knowledge gained in one circle is used to control the Utilisation and Exploitation in another circle. It is expected that if the insurance premium is to be worked out, it should be less in the second round, etc.

Step 5

Based on the observations made during the exploitation/utilisation and the qualitative data to be collected and analysed in step 4, the results shall also be used to validate the BRITS framework.

6 DISCUSSION

It is our expectation that the research at hand shall result in a set of workable guidelines/criteria that will be useful for managing ICT security in non-commercial organisations in the developing world. The second expectation is the validation of BRITS framework when applied to the non-commercial organisation in the developing world. The developing world is a part of the global network (the Internet). Possibly, given the observations made the developing world may be one of the weakest links in the Internet. This being the case, the link between the two entities through the Internet has to be studied to find out the consequences that may arise due to these differences. Interestingly, this raises the same question when linking two organisations with different security maturity levels. There are still many research questions to be discussed in reference to insuring processes included in ICT. However, in this work we build our assumptions on BRITS, where this was one of the starting points. Thus this research assumes that ICT insurance will soon be an integral part of managing ICT security risks. It is expected that the proposed guidelines/criteria to be developed will be valuable to organisations with a similar situation/environment in developing countries.

7 REFERENCES

1. [Alberts & Dorofee, 2003], Christopher Alberts & Audrey Dorofee, "Managing Information Security Risks", the OCTAVE Approach. Addison Wesley, ISBN: 0-321-11886-3.
2. [Bhattarakosol, 2003] Pattarasinee Bhattarakosol, "IT Direction in Thailand, Cultivating an E-Society. Paper Published by the **IEEE** Computer Society.
3. [Bishop, 2003] Matt Bishop, "Computer Security, Art and Science" Addison Wesley, ISNB: 0-201-44099-7.
4. [Bjorck, 2001] Fredrik Bjorck, "Security Scandinavian Style, Interpreting the Practice of Managing Information Security in Organisations. Lc.Ph. Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, Stockholm 2001
5. [Casmir & Yngström 2003] Casmir, Respickius and Yngström, Louise, "IT Security Readiness in Developing Countries: Tanzania Case Study", Published in the Proceedings of the Third Annual World Conference on Security Education and Critical Infrastructure (WISE 3), June 2003: ISBN 1-4020-7478-6.
6. [Casmir, 2003], Respickius Casmir "An Approach to IT Security Education for Developing Countries", Lc.Ph. Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, Stockholm 2003

7. [Cert, 2003] CERT/CC Overview Incident and Vulnerability Trends. Available at http://www.cert.org/present/cert-overview-trends/module-2.pdf, CERT® is a registered service mark of Carnegie Mellon University.
8. [EC46, 1995] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995.
9. [ISO/IECFAQ 2002], International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, Frequently Asked Questions. Available at http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf
10. [Klijfhout, 1996] Eric Klijfhout, "Information and Communication Technologies in the developing World, The Case of Swaziland", Twente University in the Netherlands.
11. [Kowalski, 1994] Stewart Kowalski, IT Insecurity: A Multi-disciplinary Inquiry, Ph.D Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, 1994. ISBN: 91-7153-207-2.
12. [KPMG, 2002] KPMG, "East Africa Fraud Survey 2002" Also available at http://www.kpmg.co.ke/
13. [M. Eloff & J. Eloff, 2003], M.M Eloff & J.H.P Eloff, "Information Security Management – A new Paradigm: Proceedings of SAICSIT 2003, Page 130-136".
14. [Magnusson, 1999], Christer Magnusson, "Hedging Shareholders Value in an IT dependent Business Society" THE FRAMEWORK BRITS, Ph.D Thesis, Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, Stockholm, 1999, ISBN: 91-7265-011-7.
15. [Massingue, 2003], Venancio simao Massingue, "Building Awareness and Supporting African Universities in ICT Management", THE BIG ICT FIVE (Strategy, Development/Acquisition, Implementation, Utilisation, Service Management), 2003, ISBN: 90-5271-032-5.
16. [Mbwette & Mboma, 2000] Mbwette, T.S.A and Mboma, Lucy (2000) 'Proceedings of a workshop on the Importance of a common Strategy of Information and Communication Technology (ICT) Applications in Tanzanian Universities and other Institutions of Higher Education'
17. [MEA, 2001] Esselaar, Miller and Associates, A Country ICT Survey for Tanzania Final Report, Prepared for SIDA, November, 2001.
18. [Moyo, 1996] Moyo, Lesley M (1996) Information technology strategies for Africa's Survival in the twenty-first century: IT all pervasive in Information Technology for Development v7n1 PP: 17-27 Mar 1996 ISSN: 0268-1102 JRNL CODE: ITFD.
19. [TzICT, 2003], Tanzania National ICT Policy, March, 2003.
20. [Valantin, 1996] Valantin, Robert (1996) Global Program Initiative: Information Policy Research; In Information Technology for Development v7n2 PP:95-103 Oct 1996 ISSN: 0268-1102 JRNL CODE: ITFD.
21. [Wanyembi et al., 2000], Wanyembi G., Looijen, M. "A Model For Improving ICT Management." *Proceedings of the 2000* ***IEEE*** *International Conference on Management of Innovation and Technology*, Singapore, 12-15 November, 2000.
22. [Wikipedia, 2004], http://en.wikipedia.org/wiki/Developing_countries
23. [World Bank, 2001] World Bank (2000/2001) World Development Report Attacking Poverty, Oxford University Press, USA. *Attacking Poverty, Table 19, Communications, Information and Science and Technology pp. 310 – 311.*
24. [Yngström, 1996] Yngström, Louise, A Systemic-Holistic Approach to Academic Programmes in IT Security, Ph.D Thesis, Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, Stockholm, 1996. ISBN: 91-7153-521-7.