A Holistic Approach for Managing ICT Security in Non-Commercial Organisations

A Case Study in a Developing Country

Jabiri Kuwe Bakari

Stockholm University
Department of Computer and Systems Sciences

Submitted to Stockholm University in partial fulfilment of the requirements for the degree of Doctor of Philosophy

2007

A Holistic Approach for Managing ICT Security in Non-Commercial Organisations
-A Case Study in a Developing Country

Doctoral dissertation
Stockholm University/Royal Institute of Technology
Department of Computer and Systems Sciences
Stockholm, Sweden

Report series: DSV No. 07-003
ISBN 91-7155-383-8
ISSN 1101-8526
ISRN SU-KTH/DSV/R-07/3-SE

Printed by
Universitetssevice US-AB, Stockholm, Sweden, 2007

Abstract

The use and development of Information and Communication Technology (ICT) has improved the efficiency and flexibility in providing services. While computerisation is taking place at a fast speed, the security of critical ICT assets is a growing concern for management. This is because the potential for financial damage is intensified and may result in the loss of strategic information and property, in service interruption and liability claims. If these risks are not taken care of, the objectives of organisations might be negatively affected as well.

The research reported here is about improvement of the ICT security management process in non-commercial organisations in order to reduce possible financial damage, taking into consideration the realities found in developing countries. The research took place in a developing country—Tanzania, where five organisations were involved. The data gathering instruments employed were questionnaires with multiple choice questions, open-ended questions, and face-to-face interviews with some selected respondents. Also, onsite observation (participatory) and documentary review was used. The respondents were mainly senior management, Operational managers, IT Managers and system administrators, and general and technical staff.

This thesis presents the empirical investigations and analyses carried out in the organisations. The study is organised into seven papers covering: the state of ICT security management in the organisations; prerequisites when utilising the existing ICT security management approaches in attaining a solution for managing ICT security in the organisations; issues and challenges of managing ICT security; important aspects to be taken into consideration in order to successfully manage ICT security; and how the management of ICT security in non-commercial organisations could be improved. Among others, the research was motivated by the observed need for bridging the perception gap between the management and technicians when dealing with the ICT security problem, and consequently extending to a common understanding by the staff in the various departments and specialities within and between the departments.

The thesis contributes to increased empirical knowledge on the importance of the holistic ICT security management process. Particularly, our main contribution is the proposed holistic approach for managing ICT security in non-commercial organisations, organised in the form of guidelines with two main phases: the initialisation phase which involved the introduction of the ICT security management process in the organisation; and the internalised and continuous phase. The research confirmed that the backing of general management and staff is important for the success of the ICT security management process in the organisation. This implies that the management allows the organisation through its own acquired knowledge and confidence, to internalise the ICT security management practices, thus enabling people to act confidently at all levels. Knowing about the ICT risks and their consequences for the core service operations of the organisation, the management and staff at all levels and from all departments or specialities are more likely to offer their support to ICT security endeavours.

Acknowledgements

First I would like to thank my supervisors, Professor Louise Yngström and Dr. Christer Magnusson for their constructive advice and guidance throughout this research work. My thanks also go to Professor Beda Mutagahywa of the University of Dar es Salaam Computing Centre for his valuable advice and comments, in particular, during my research activities in Tanzania.

Secondly, I would like to take this opportunity to thank my colleagues at the Department of Computer and Systems Sciences (Stockholm University and Royal Institute of Technology) Security Lab, for their valuable input and discussion during the research process, especially Charles Tarimo, with whom I have shared many insights and discussions; also Mengistu Kifle, Jeffy Mwakalinga, Fredrik Björck and Job Chaula. I extend my thanks to Deogratias Fuli and Masoud Mahundi of the University of Dar es Salaam for assisting me during the data collection and in particular the pilot survey. I would further like to thank all the individuals and organisations in Tanzania that assisted in making this research possible, as well as the respondents for the time and effort they took to answer the questionnaires and to participate in the interviews to provide me with the research data and hence empirical foundation of this thesis. In particular, I would like to extend my thanks to the Senior Management of the five studied organisations in Tanzania for giving me the opportunity to carry out my fieldwork in their organisations and graciously sharing their experiences with me.

Thirdly, my thanks go to Prof. Francis J. Sichona and Dr. Lucy Mboma of the University of Dar es Salaam for introducing me to research methodology, and to Mrs. Graham Wilson for checking the English of this thesis at an early stage. Any new mistakes are entirely mine. Also I am especially thankful to Birgitta Olsson, Fatima Santala and Rodolfo Candia of DSV-SU/KTH for handling administrative matters during the research process.

There are many others who contributed to this thesis in one way or another and I wish it would have been possible to list you all. All those I met during the research process, relatives, friends and colleagues I appreciate your contributions and I thank you all.

Fourthly, I am very grateful to the Swedish International Development Agency (SIDA)/ SAREC for funding this research work and the University of Dar es Salaam for granting me the opportunity and by giving me study leave.

Special thanks to my wife, Amina, for her love, support, patience and for taking care of our daughters Zuhra, Warda and our newly born Nahya, during the whole period of the research, especially during the months I spent away.

Finally, I would like to say Thank you God that, through you, all this has been possible. The doctoral process has taught me not only about research, but also about myself, people and the world.

Dedication

To my late Dad

Table of Contents

Part I - Prologue

Part II – Publications

Part III – Appendices

List of Figures

List of Tables

List of Abbreviations

ALE	Annual Loss Expectation
ATM/POS	Automated Teller Machine/Point of Sale
BRITS	Business Requirements on Information Technology Security
BS	British Standards
CC	Common Criteria
CCTV	Close-Circuit Television
CEO	Chief Executive Officer– Used in this study to mean people in the top senior position
CFO	Chief Financial Officer
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and related Technology
EASSy	East African Submarine Cable System
EMitL	Estimated Maximum information technology Loss
GDP	Gross Domestic Product
GST	General Systems Theory
ICT	Information and Communication Technology
ICTs	Information and Communication Technologies
IDSs	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IS	Information Systems
ISACA	Institute of Information Systems Audit and Control Association
ISMS	Information Security Management Systems
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	IT Infrastructure Library
KPIs	Key Performance Indicators
MSS	Managed Security Services
MSSP	Managed Security Service Provider
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OECD	Organisation for Economic Co-operation and Development
OFC	Optic Fibre Cable
PCs	Personal Computers
PDCA	Plan-Do-Check-Act
SBC	Security By Consensus
SONGAS	Songosongo Gas Supply
TANESCO	Tanzania Electric Supply Company
TAZARA	Tanzania Zambia Railway Authority
TCRA	Tanzania Communications Regulatory Authority
TRC	Tanzania Railway Corporation
TTCL	Tanzania Telecommunication Company Limited
UDSM	University of Dar es Salaam
VLANs	Virtual Local Area Networks
VPN	Virtual Private Network
ZANTEL	Zanzibar Telecommunication Limited

Part I

Prologue

Chapter 1

1. Introduction

The use and development of Information and Communication Technology (ICT) has improved the efficiency and flexibility in providing services and many organisations today are increasingly relying on ICT which evidently handles a very critical part of the organisations' core services. While computerisation is taking place at a fast speed, the security of critical ICT assets is a growing concern for management, because the potential for financial damage is intensified and may result in the loss of strategic information and property, and in service interruption, which can lead to liability claims. If these risks are not taken care of, the objectives of these organisations might be negatively affected as well. This work is about the improvement of the ICT security management process in non-commercial organisations in order to reduce financial damage, taking into consideration realities found in developing countries.

ICT encompasses everything used in modern communication and knowledge transmission. The components of ICT are as follows; Hardware: This includes machines or equipment like phones, computers, routers, switches, TVs, fax, etc., as well as the infrastructure like landline cables, microwave systems, radio transmitters, satellites and satellite ground stations, fibre optic cables, etc. Software[1]: This includes operating systems and application-software[2]. ICT also includes Data and Information being stored, processed, and exchanged; Human expertise, which is needed to design, plan, install, operate, manage, control and maintain hardware, software and data or information. Finally procedures are required to make use of the functionality of the Hardware, Software and Data or information (Alberts & Dorofee 2003).

1.1 Background

The use of ICT has led to tremendous changes in the economy and even the way people live. However, in the developing world[3] the use and development of ICT capabilities is still limited and faces a wide range of constraints and challenges (Moyo, 1996; Klijfhout, 1996; Straub, 2001; Bhattarakosol, 2003; Chaula, 2006; Tarimo, 2006; Gelan, 2006). These constraints include issues such as poor or lack of infrastructure, social problems, and the lack of an appropriate legal, political and economic framework. Others are absence of ICT policies, implementation procedures, a general lack of appropriate knowledge of ICT among suppliers, managers, planners

[1] Set of Instructions
[2] Information systems and programs which make everything work to fulfil certain requirements
[3] According to (Odedra & Madon, 1993), developing countries or least developed countries are those countries which are in the process of becoming industrialised but have constrained resources.

and users, and few trained or skilled ICT personnel. Such problems lead to many challenges, especially for management when it comes to implementation in particular, as well as control and maintenance (Looijen, 1998). Moyo (1996) and Valantin (1996) point to the poor infrastructure, especially communication infrastructure, limited 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 of ICT is not being transferred at the same speed as the technology itself.

These challenges and constraints manifest themselves at the organisational level. Wanyembi et al. (2000) point out that the rapid diffusion of ICT in many organisations in developing countries is a new and growing phenomenon, which presents serious challenges. They further assert that, while vast amounts of hardware and software are acquired in increasing quantities, users' expectations of improved services are not being fulfilled, partly due to the poor quality of management and maintenance of ICT. Literature and experience suggest that in many organisations in the developing countries, deployment of ICT is not part and parcel of organisational reform or business re-engineering (Mhayaya 2003; Bakari, 2005). My experience is that very little or no attention at all is paid to how to use ICT. In some instances, users have expressed frustration due to unfulfilled expectations of the performance of the new technology. In order to address these challenges, organisations in developing countries are attempting to use existing solutions[4] that promise to solve these problems, which are similar to those found in the developed world. However, a 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; Klijfhout, 1996).

Of particular interest here is the problem of ICT security. The development of information and communication technologies (ICTs) has gone hand in hand with the emergence of new types of vulnerabilities and threats. The ICT security problem encompasses any deliberate act affecting three fundamental properties of an information system. These properties include confidentiality, i.e. a computer system's or network's ability to store sensitive information in a secure manner and to maintain exclusive access to designated users; integrity, i.e. the assurance that programs and data or information are designed and modified only in an authorised manner, and hence reliable; and availability, i.e. continuous accessibility and service of the computer system or network to users without delays or blackouts. This problem can affect individual users, small and large organisations and governmental services, and have financial implications too, for example, direct costs, such as the theft of money, digital assets, or sensitive information. It can also cause indirect costs in the form of service interruption, legal liability, and lower productivity due to diverted resources such as personnel, capital, bandwidth and computing power, etc., which can further lead to costs related to the long-term impact of an attack on brand image, bad reputation, competitiveness, and financial markets (OECD[5] 2006).

[4] Existing solutions here means various frameworks, models, standards and best practices

[5] Organisation for Economic Co-operation and Development

Despite the constraints mentioned above, organisations in developing countries are now undergoing radical transformation to embrace the "information age". This makes them start relying heavily on ICT evidently to handle a very critical part of the organisations' core services, and consequently a valuable asset of the organisation—information.

The point of focus here is the management of ICT security, which should be part of risk management. This is due to the fact that information is a valuable asset and should be protected appropriately. ICT security management is the overall process of establishing and maintaining adequate ICT security within an organisation in order to achieve and maintain appropriate levels of confidentiality, integrity, availability of information, information systems and services. The study of ICT security management is wide and is applicable to all types of organisations worldwide. Our intention in this research work is to assess the current state of ICT security management, using example of non-commercial organisations in Tanzania[6] and to uncover the likely problems and potential consequences arising from ICT risks. Hence we sought to capture top management[7]'s attention about the problem of ICT security in their organisations, and later to suggest ways to improve it. The non-commercial sector was selected because it would be feasible to get the required information for the research since most of these are government organisations and so they are public.

1.2 Problem area

Despite the problems of ICT security outlined above, the dependence on ICT to operate core services in the organisations is increasing rapidly (Bakari & Mboma, 2001; Bakari, 2005; Mbwette & Mboma, 2000; MEA, 2001; Mhayaya, 2003; Sulla, 2004; Tarimo, 2006). The focus of organisations in Tanzania is on what is commonly known as "Computerisation" (Bakari et al., 2004). Very little or no attention at all is paid to the procedures on how to securely use ICT. This is partly due to the following reasons:

(a) Not knowing that they are vulnerable to ICT-related risks as a result of computerisation and those who do know have no idea to what extent they are exposed to these risks nor how to go about addressing the problem apart from employing technical measures which are also on an ad-hoc basis. ICT security is not seen as a risk to the organisation's business.

(b) A relaxed culture and lack of formal ICT and ICT security policies, procedures and their operationalisation. One may argue that there are a number of technical solutions available ranging from anti-virus, firewall to intrusion detection systems, and indeed there are organisations which have deployed some of these solutions,

[6] Is one of the developing countries, situated in Sub-Saharan Africa – Attained her independence in 1961- Tanzania is the biggest of the East African countries with an approximate area of 945,000 km^2 and estimated population of 33 million people according to the 2002 census and an average growth rate of 2.8%. About 50% of the population is living below the poverty line. Per capita Gross Domestic Product (GDP) is estimated at US$ 251 (2001) (Tanzania, 2005). See also state of ICT in general in appendix F

[7] Top management is used here to mean strategic level management

but due to lack of guidelines about proper usage and management, the problem is left to suppliers/vendors of ICT. A small number of staff with no ICT security training also amplifies the problem.

(c) Believing that ICT security is a technical problem and therefore both ICT in general and ICT security in particular being set aside for more important things. For example, in the first phase of this research, we found that there is a perception gap between the management and the technical personnel whereby the ICT security problem is perceived by the general management as a technical problem rather than as a risk, preventing the organisation from meeting its objectives. As a result, measures for ICT risk mitigation that are ultimately put in place in such organisations tend to be inadequate and mostly technical, believing that anti-virus software and "top-of-the-range" firewalls are sufficient.

(d) Complexity of the existing solutions and not knowing where to start. For example, the existence of best practices and standards such as ISO 17799 or BS 7799 may not be easily adopted directly by organisations in the studied environment[8] which are in particular at the take-off stage as far as ICT is concerned without some sort of interpretation and guidance. The standard itself suggests that it should be carefully tailored to the specific requirements of the adopting organisation.

> "*ISO/IEC 17799 does not provide detailed conformance specifications necessary for an organisational information security management program. It does not provide enough information to support an in-depth organisational information security review*".
>
> *November, 2002* (ISO/IEC 17799:2000)

There is therefore enormous potential for damage, which may result in loss of strategic information, service interruption and loss of property which could lead to liability claims, all of which have negative effects on the organisation's mission with financial implications.

1.3 Purpose of the Research

The *purpose* of this research is to suggest ways on how the management of ICT security can be improved in order to reduce the potential financial damage as a result of computerisation in non-commercial organisations. This was achieved through a number of stages namely:

- to investigate the current practice of ICT security management in non-commercial organisations;
- to explore the existing ICT security management approaches in order to investigate their applicability in attaining a solution for managing ICT security in non-commercial organisations;
- to investigate the issues and challenges to be addressed in the initial stages of computerisation; and
- to explore the important aspects to be considered in order to successfully manage ICT security in the studied environment.

[8] Studied environment refers to Tanzania

Such steps or suggestions shall be based on the existing and accepted theories in conjunction with other assumptions and models as also suggested by Kuhn (1962).

Given the above observations of the problem, our intention then was not just to develop another security management approach, not just another model or framework. As detailed in chapter 3 and with reference to Baskerville (1988) and Zuccato (2005), security management approaches have evolved from first generation to sixth generation, the latter ones being holistic approaches. Such approaches include Business Requirements on Information Technology Security (BRITS[9]) framework - (Magnusson, 1999), Security by Consensus (SBC) model - Kowalski (1994) and Holistic Information Security Management Framework (HSMF) – Zuccato (2005). In addition there are also standards and best practices such as ISO17799, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE[10]) - Alberts & Dorofee (2003), Control Objectives for Information and related Technology (COBIT[11]) – ISACA (2005), IT Infrastructure Library (ITIL) – ITIL (2005), and Outsourcing to a third party organisation called a Managed Security Service Provider (MSSP) - Allen et al., (2003). It was therefore important to first explore these existing ICT security management approaches to investigate their applicability in attaining a solution for managing ICT security in non-commercial organisations. Since the ICT security management problem exists in the real world and it is not practical to study the whole world, an instance was identified as a representative of the real world. Figure 1-1 presents the proposed research set-up.

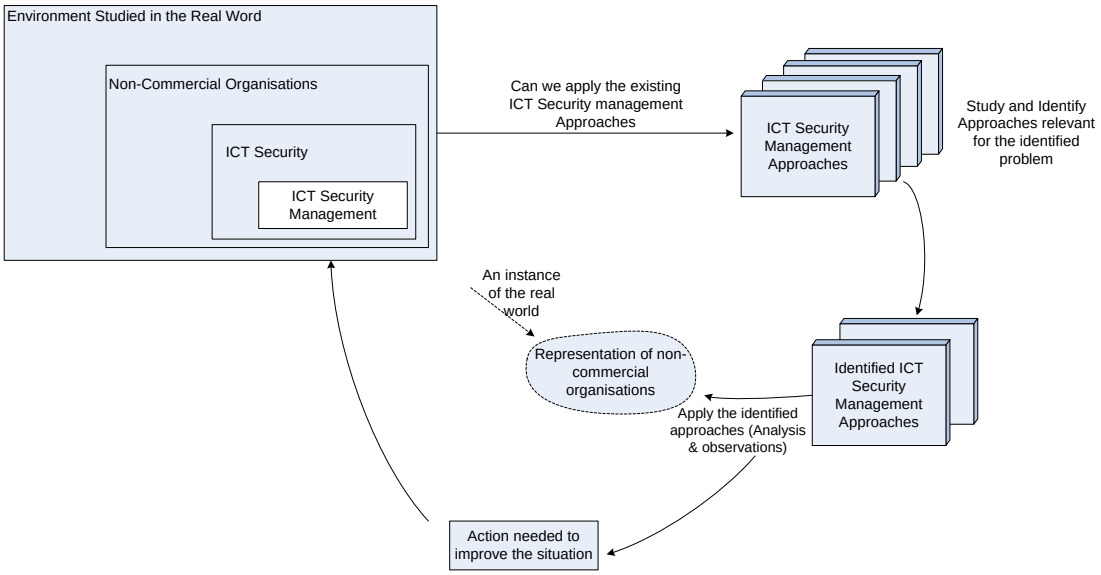


Figure 1-1: Proposed Study setup

For our work, non-commercial organisations were identified for study purpose, and which brings us to the *focus* of this research—non-commercial organisations, i.e. organisations that are not profit making but have an obligation to deliver services.

[9] BRITS framework attempts to bridge the gap between top management and IT personnel. It translates the financial language to the IT and IT security languages, and vice versa.

10 OCTAVE is a risk-based strategic assessment and planning technique for ICT security, and was developed at the CERT Coordination Centre (CERT/CC).

[11] COBIT has been developed by the IT Governance Institute of Information Systems Audit and Control Association (ISACA).

Such organisations include government institutions like public universities, National Social Security Funds, Airport Authorities and public healthcare. Many of these organisations have become increasingly dependent on ICT-platforms, and hence more exposed to ICT-related risks (Mhayaya, 2003; Sulla, 2004; Chaula, 2006; Tarimo, 2006). If these risks are not taken care of, the objectives of these organisations will be affected negatively. While in commercial organisations the main objective is to hedge shareholder value, in non-commercial organisations the main objective is to fulfil the organisation's missions—to deliver services such as education and healthcare services within the budget of the organisation. Although in non-commercial organisations the objective is not to make a profit, risks associated with ICT use have financial implications too. This is due to the fact that the ability of any organisation which depends on ICT to operate its core services, to achieve its mission and meet its business objectives is directly linked to the state of its ICT infrastructure (Alberts & Dorofee, 2003). Therefore, in order to ensure that the non-commercial organisations meet their objectives, there must be proper and continuous ICT security management.

When a commercial organisation suffers a loss due to an ICT security problem, for example, the market can make decisions to have the company go bankrupt! However, one cannot close a non-commercial organisation like a public university or a government ministry because of a loss associated with an ICT security problem. An example of 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 service or service interruptions. The value of the research at hand is to improve the ICT security management process in order to reduce such consequences.

1.4 Motivation

Having worked in the field of ICT for more than six years, holding different positions, participating in, coordinating and supervising various ICT projects, I have experienced for example how the deployment of ICT at the University of Dar es Salaam (UDSM) has changed it in many ways and well beyond my imagination, compared with the time when I was admitted to the University in 1993 as an undergraduate student. Faculties have the opportunity to significantly change the traditional teaching and delivery processes. Collaboration has been developed within and beyond the classroom. Administration of various University processes such as Financial Information system, Academic Registry Information system and Library Information system has been considerably eased and the University leads the way and has gained a nationwide reputation in the area of ICT, in particular for promoting the appropriate use of information technologies to support and improve learning, teaching, research and administration.

However, several trends can be identified which made us doubt the sustainability of ICT use at the University in particular and the country in general. For example, the number of reported incidents of breaches in security is on the increase, whereby huge sums of money are said to have disappeared or been stolen through computer fraud.

An example of such reports 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 potentially at risk. The number of fraud cases as reported in (Chaula, 2006), and the theft of Tanzania shillings 300 million from the Prime Minister's office as reported in (Tarimo, 2006), are a few examples that can be mentioned.

Another example is that of auditing and lack of management support. In the study "The impact of Information Technology on Internal Auditing in Tanzanian Organisations" by (Chacha, 2000), there is indication that the auditing process in the organisations is facing a big challenge as computerisation increases. Auditors use directives and principles laid down for manual performance. The study shows that almost all internal auditors in the surveyed organisations are still using the same techniques and tools when auditing computer-based systems as they used when these were performed manually. This means auditing around the computer. The two studies (Suluo, 2003) and (Chacha, 2000) point to the lack of management support as a hindrance to successful use of ICT in Tanzanian organisations. Mhayaya (2003) studied the implementation of ICT in government organisations and came up with many problems, including the low level of ICT literacy in society at large and the government in particular and a lack of clear coordination among ICT professionals in the government, industry and the private sector. Mhayaya argues that although there have been remarkable achievements in ICT usage, there is still a problem on the part of ICT management. There are no plans and no formal training in many organisations. Instead, the issue of training is left to the employees themselves and as a result most of them fail to gain the knowledge needed for ICT applications in the organisations where they work. Mhayaya also argues that low transformation effectiveness is due to lack of business process re-engineering and strategic planning, which could also be attributed to the lack of qualified senior personnel who are given the mandate of managing the ICT resources. In this context, there is a need to challenge the 'non-crisis' management approach to one of 'crisis management', being prepared for every unforeseen eventuality.

Another problem is that of culture. Based on my own experience and being part of the society, I can describe Tanzanians as characterised by generosity that affects not only material exchange, but also information exchange. Because of this generosity, you may ask to know about one thing and end up with a lot more information being provided. One with malicious intention may benefit from the extra information and even the sincere, with kindness, may be tempted to misuse the information. Such social engineering[12] techniques might be a big problem in this environment. In this case, despite applying all known technical and non-technical measures to secure information systems in an organisation, security becomes the issue of how easy it is to gain employees' trust. Unfortunately, even in organisations with state-of-the-art security solutions in place, serious occurrences of penetration happen through social engineering, simply because of the kindness and openness of the people (Granger, 2001). Furthermore, in connection with culture was the observed lack of discipline

[12] Social Engineering involves the exploitation of human vulnerabilities, such as ignorance and an individual's natural desire to be kind and helpful. The goals of social engineering are the same as in hacking, i.e. to gain unauthorised access and cause insecurity. Social engineering takes advantage of trust, which is one of the weakest links in the security chain, taking into consideration the natural human tendency to accede when someone verbally requests something.

concerning password which appears to be a very significant problem. It is very common to have passwords shared among employees. This is not a good situation. A number of researchers such as Bishop (2003), Caelli et al., (1991) have already indicated that threats come from inside. Therefore measures such as efficient access, authentication, non-repudiation type of controls and audit trails together with specialised training and awareness programmes, should be introduced.

There is also an indication that most people in the studied environment tend to value tangible things like PC hardware, but not the information in it. In the same way people working in the registry where they take care of the confidential physical files of the organisation are properly vetted, while the systems administrators are not. There is therefore a need to change the culture as we enter the information economy to reflect contemporary economic trends.

However, not all the above-mentioned problems are due to security failure or may cause security failure. Security may form one factor that hinders sustainability.

As pointed out in section 1.2, despite the many problems as outlined above, the speed of deployment and use of ICT has been dynamic. For example, according to a speech[13] by the Minister of Communication and Transport (MoCT), the country already has 2 Public Switched Telephone Networks namely TTCL and Zantel, as well as the availability of 4 Mobile Cellular Network companies**,** 11 data communications network companies, 9 Private data communications networks**,** 21 Commercial internet service providers and thousands of internet cafes. The speech also highlights the number of users of mobile phones as follows; Vodacom (700,000 users), Mobitel[14] (220,000), TTCL (160,000), Celtel (350,000) and Zantel (70,000) adding up to 1.4 million users in June 2004 as compared with a total of 850,000 users in June 2003. Almost the entire country is covered by mobile phone operators. Figure 1-2 shows the exponential increase of mobile telephone subscribers. The small number of fixed line subscribers may be due to the poor infrastructure.

[13] Minister's speech: 2004/2005 budgetary speech for the Ministry of Communication and Transport.
[14] Recently changed its name to Tigo

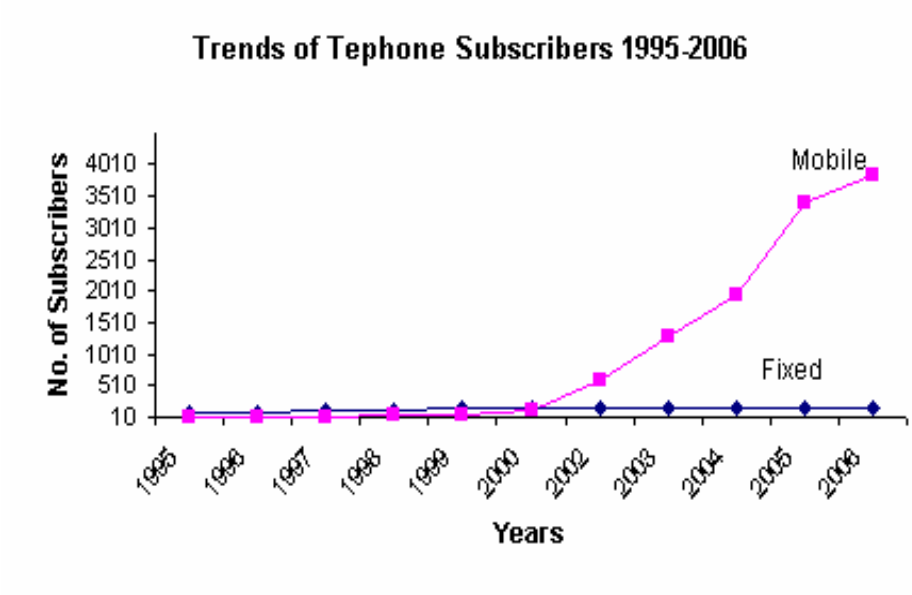


Figure 1-2: Trend of Telephone Subscribers in 1000s: 1995-2006 – Tanzania (Source: TCRA, 2006)

At the organisational level, computerisation of core business operations is advancing. At the national level, a national ICT policy was put in place (in 2003) and various organisations in the public and private sector are now in the process of computerisation. There are number of initiatives at the national level including, for example, the Agricultural Management Information Database, Land Management Information Database, The Tanzania Inter-Bank Settlement System, Natural Resources and Tourism Management Information System, Customs Administration System (ASYCUDA++), Online Motor Vehicle Registration System, Strategic Budget Allocation System (SBAS) for the Ministry of Finance, By-Law making database for Local Authorities. Education Management Information System, The Local Government Monitoring Database, Integrated Financial Management System, an accounting system for central and local Governments, Integrated Payroll and Human Resources Information System, Planning and Reporting (PlanRep) Database in the Local Government Authorities throughout the country, Integrated Statistical Database, and the recently proposed National Identification Card Project under the Ministry of the Home Affairs, just to mention a few. In addition, most of the financial institutions, such as banks, are computerised, with the introduction of Automated Teller Machines (ATM) and Point of Sale (POS) machines.

However, these information systems are being implemented as islands of information systems that are not integrated, partly due to the absence of policy operationalisation and directives. Another problem is that of lack of awareness of the consequences to these types of data if they were compromised. The absence of an ICT usage policy and procedures in most organisations allows users to make their own decisions on how to handle and use the organisations' ICT assets.

These and other observations made by (Mbwette & Mboma, 2000; MEA, 2001; Bakari & Mboma, 2001; TzICT, 2003; Tanzania, 2005) show how fast the dependence[15] on ICT is growing on a daily basis and hence the exposure to ICT-related risks.

[15] See appendix F for more information on ICT in Tanzania

My observation, both within and outside the University, is that there has been a trend in many organisations, including government institutions, to concentrate on and pay more attention to design, procurement and deployment of ICT, but without taking into consideration the usage and operational procedures. In other organisations even the IT department was missing and therefore basically ICT-related issues were nobody's responsibility, while in other organisations some units make their own arrangements on the design, procurement and deployment of ICT. In some instances, the philosophy was, "Buy the computer or install the network and then start thinking about what to do with it". Staff are given no preparation. While (Magnusson, 1999) argues that sub-contractors', suppliers' and consultants' access to important ICT resources is generally a weak link in security, in Tanzania ICT suppliers and vendors in many instances can somehow control the supply, installation and maintenance process.

In the first place, a general observation shows that organisations in Tanzania, regardless of their size, acquire, adopt and use the new technology, while computer abuse and breaches of security of information systems are increasing, not only within Tanzania but also worldwide. Figure 1-3 below shows that the problem of insecurity is growing exponentially worldwide. While the rate at which new vulnerabilities are discovered continues to increase, the volume of reported incidents is also increasing as reported in the most recent Computer Crime and Security Survey by Gordon et al. (2006).

Figure 1-3: Trend of reported incidents worldwide, Source: (Cert, 2005)

ICT security-related cases are not going away and are expected to increase further as the computer literacy rate improves. Predictably, for Tanzania, 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 controls. ICT security control weakness in the studied environment has the potential of being the weakest link on the Internet. This may affect negatively the ongoing efforts of trying to bridge the existing digital divide between the developing and developed countries. I think that the developing countries do not intend to go through the 20 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 20 years. This being the case, ICT weakness in the developing world has the potential of being the weakest link on the Internet.

Secondly, many non-commercial organisations in Tanzania are at the stage of migrating from non- or semi-computerisation for some core services to the point where they will fully depend on ICT. While this is the only way forward in improving the services, from a security point of view it is considered as non-secure migration as depicted in figure 1-4. In the figure, dotted lines indicate that the integration of ICT in core business for the developing countries was slow and in same case started at later stages with fast growing.

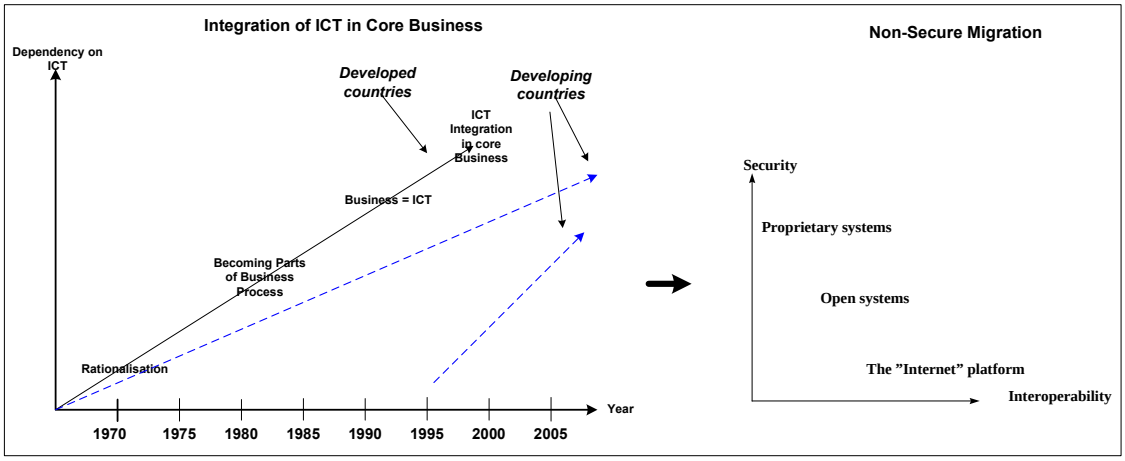


Figure 1-4: ICT's Integration in Core Business Vs Non-secure migration: Based on (Magnusson, 1999)

It is therefore important for the stakeholders to be made aware of the ICT-related risks that organisations are exposed to as they migrate, their consequences and how to handle them.

The point I would like to emphasise here is, while ICT security is a growing concern, it is not receiving its due attention particularly in the area in focus. It is important to explore these issues at an early stage in the development of ICT, as it might otherwise be complicated and expensive to address the ICT security management problem at a later stage. These reasons motivated me to investigate the ICT security management problem in more detail with an attempt to address the *perception problem* a*nd suggest ways to improve the management of ICT security, particularly in non-commercial organisations*. This brings us to the following section—research questions.

1.5 Research Questions

The research presented in this thesis addresses the main research question below and was conducted by carrying out five studies.

How could the management of ICT security in the non-commercial organisations be improved in order to reduce the potential financial damage as a result of computerisation?

In order to address the main research question, we had to go through five stages which resulted in 5 studies[16] and further sub-research questions, all directed towards the main research question as follows:

Stage 1: We first needed to get an indication of the problem. This involved finding out the current practice of ICT security management in non-commercial organisations in the studied environment and to what extent the organisations in the studied environment depend on ICT to run their core services. Furthermore, it was equally important to uncover the likely problems and potential consequences arising from ICT risks as the dependency of organisations' core services on ICT grows. This was achieved through research question 1

Res.Q.1 *What is the current practice of ICT Security management in organisations in the studied environment? → Indication of problems*

The answer to this question is presented in **PAPER I**, where the state of ICT security management is discussed.

Stage 2: The problem of ICT security management is not new. It has been around for some time. A number of ICT security management approaches exist, such as OCTAVE, BRITS, ISO17799, COBIT, IT Infrastructure Library (ITIL), Security by Consensus (SBC) and Outsourcing to a third party organisation called a Managed Security Service Provider (MSSP), to mention a few. Thus it was relevant to identify what these solutions are, how they work and what are the prerequisites if we are to use them, and finally whether there is any appropriate solution for the identified problem, and if so, then apply it.

Res.Q.2 *What are the prerequisites when utilising the existing ICT security management approaches in attaining a solution to the identified ICT security management problem?*

[16] Summarised in figure 1-6

In **PAPER II**, a discussion on an attempt to utilise one of the frameworks, namely BRITS is presented. Furthermore, **PAPER III** discusses when outsourcing the ICT security approach is used as a solution to the identified ICT security management problem.

Stage 3: One of the findings in our initial stages of the research was that organisations in the studied environment are in the initial stages as far as computerisation is concerned. This prompted us to find out the issues and challenges to be addressed in the initial stages of computerisation as suggested in the following research question.

Res.Q.3 *What are the issues and challenges to be addressed in the initial stages of computerisation, from an ICT security point of view?*

The answer to this question is presented in **PAPER IV,** which attempts to underline the issues and challenges of the emerging computerisation in the developing countries, taking the instance of the e-government systems from an ICT security point of view.

Stage 4: Following the observations of the state of ICT security management in study 1, the prerequisites when utilising the existing solutions in study 2, and the issues and challenges to be addressed in the initial stages of computerisation from an ICT security management point of view in study 3, the next concern was what else needed to be observed in order to successfully manage ICT security given the developing environment. This led us to the fourth research question.

Res.Q.4 *What are the important aspects to be taken into consideration in order to successfully manage ICT security? → Given a developing environment with respect to ICT, what else needed to be observed?*

The answer to this question is presented in **PAPER V**, where an attempt to address the important aspects in the process of attaining, developing, implementing, and managing ICT security in organisations is presented.

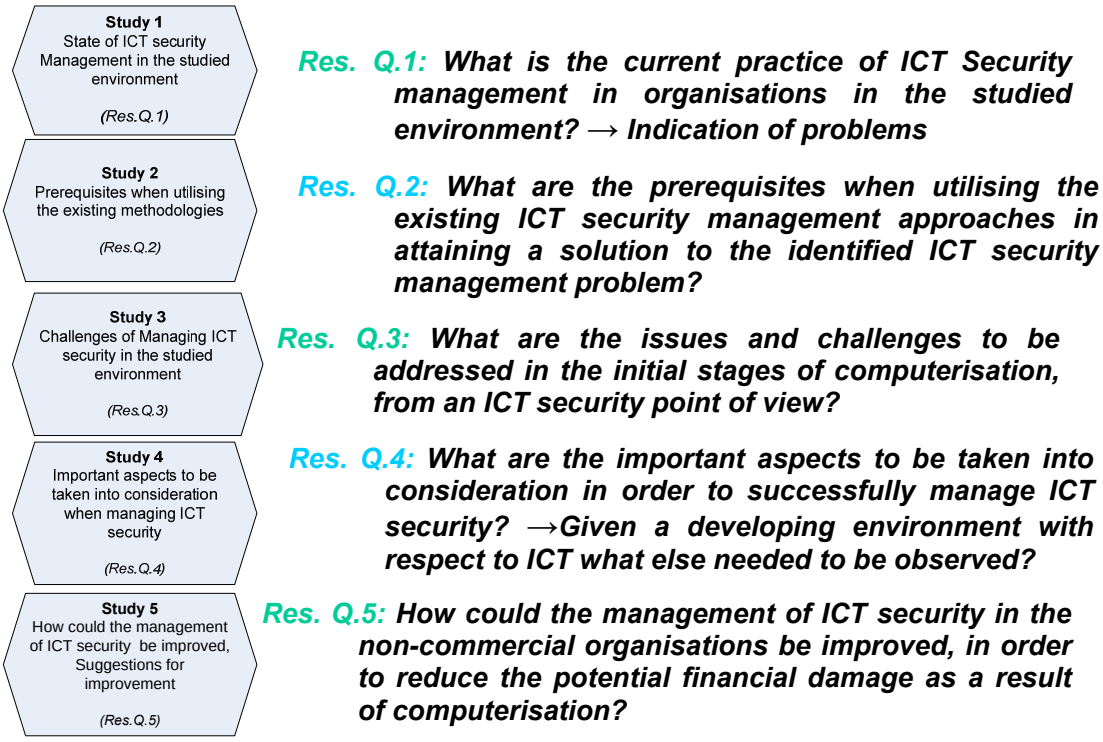
Stage 5: Based on the findings from the four stages above, we were then in a position to answer the main research question.

Res.Q.5 *How could the management of ICT security in the non-commercial organisations be improved, in order to reduce the potential financial damage as a result of computerisation?*

In **PAPER VI,** 10 steps on how to bridge the perception gap between the general management and technicians are presented. This was part

of the improvement of the ICT security management process. Based on the observations made in this study and studies 1-4, a holistic approach to address the problem was proposed as presented in chapter 4.

Below we present the summary of the five studies and their respective research questions.



1.6 Research Evolution

In this section, we briefly describe how the research presented in this thesis evolved. Generally, it started with Problem observation → *then we consulted* Theory → *back to Practice, observe* → *consult* Theory *again*→ *back to* Practice, observe again → *and* finally back to theory again with contribution.

The entire research work can be summarised into five circles, each characterised by Reflection-Planning-Action-Observation and then reflection again for the next circle as show in figure 1-5. The actual involved processes are summarised in figure 1-6. In the first circle, we conducted a literature review to identify the issues surrounding ICT implementation and their impact on the developing world in general and on Tanzania in particular.

From this review, ICT security management was identified as one of the prime problems that need immediate attention. This led us to further review the literature on the theory behind the ICT security management process and the various approaches to it, the details of which are presented in chapter 3.

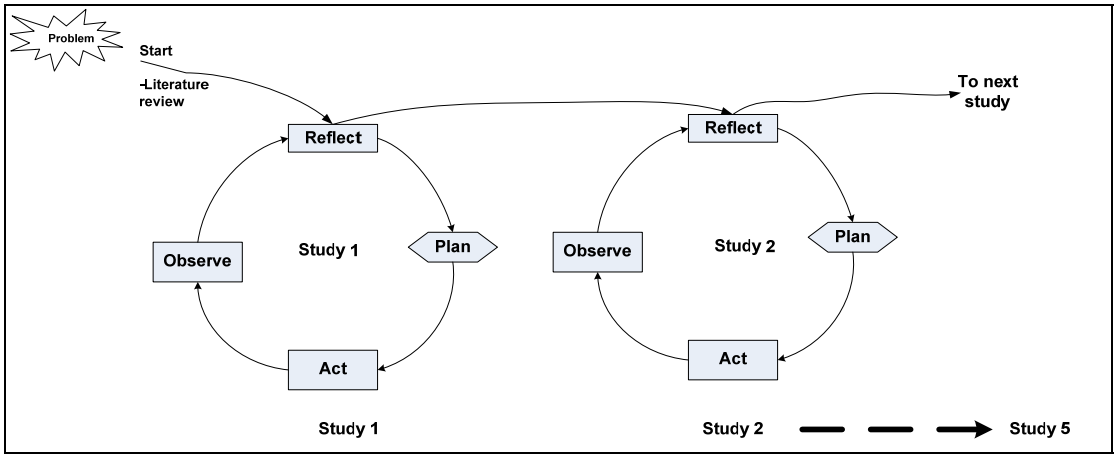


Figure 1-5: Research Paradigm

Since it was not feasible to study the whole world, five non-commercial organisations were identified[17]in Tanzania for more detailed and informative research about the identified ICT security management problem. In order to get an indication of the magnitude of the problem, a study[18] referred to as **study 1** was conducted in those five non-commercial organisations in order to find out the current practices of ICT security management in the studied organisations, thereby uncovering possible serious problems.

This first circle of our research was concluded by reflecting on the results we got from **study 1** and a further literature review of the two main issues. First, ICT security management approaches were reviewed to determine whether there were any that would be relevant for the identified problem in **study 1** and whether they would be suitable for the non-commercial organisations in the studied environment[19]. As pointed out earlier, it was not our intention to just create another model or framework. Instead it was relevant to review the existing approaches in order to find out if one exists that can address the identified problem. This review led to **study 2**[20], which involved the application of identified ICT security management approaches to the identified problem and which also resulted in the *validation* of the identified approaches when applied to the studied environment. This marks the first main contribution of this thesis as detailed in sections 5.2 and 5.3. The second issue, which came immediately after the first circle, involved a review of the issues surrounding ICT security management implementation, given the observed state of ICT security management in **study 1**. These reviews led to **study 3**[21] and **study 4**[22]. In **Study 3**, issues and challenges to be addressed in the initial stages of computerisation, from the ICT security point of view, are discussed. Furthermore, the important aspects to be taken into considerations in order to successfully manage ICT security, given the developing environment with respect to ICT, are discussed in **study 4**.

[17] See the details of the five organisations and research methodology in chapter 2
[18] See Study 1 and paper I
[19] The phrase “studied environment” is used here to mean Tanzania
[20] See study 2 and Paper II & III
[21] See study 3 and Paper IV
[22] See study 4 and Paper V

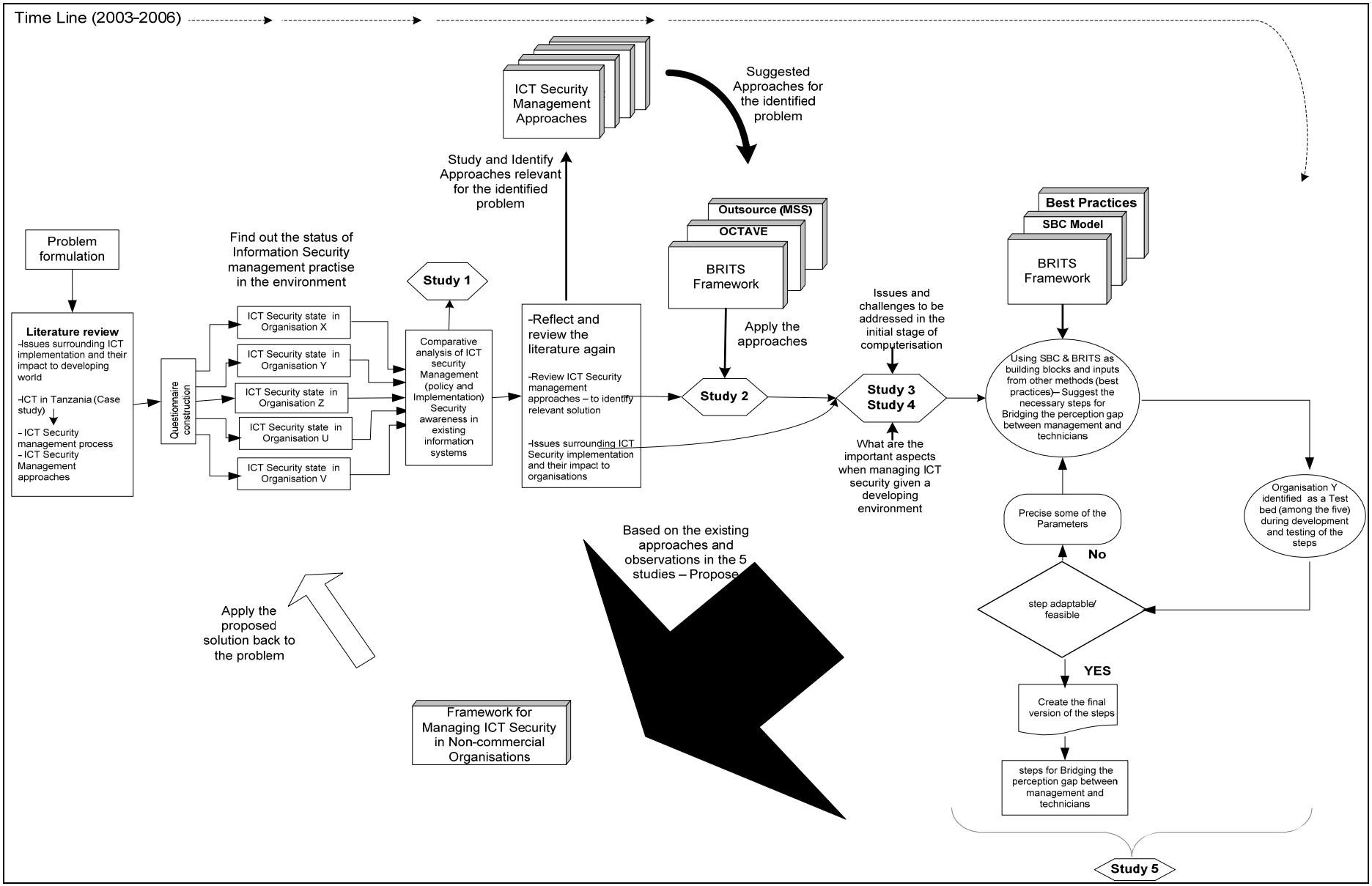


Figure 1-6: Research Evolution

One of the major observations in **study 1** and in the reviews was the presence of the perception gap problem between the general management and technicians when it comes to addressing or dealing with the ICT security management problem in their organisation. This problem was partially addressed in **study 2**, which however indicated major prerequisites as pointed out in the study for the identified approach to address the existing ICT security management problem as indicated in **study 1**.

These observations and others made in studies 3 and 4 on the issues surrounding ICT security management implementation in the studied environment indicated the need for another study which could address the perception problem and hence improve the ICT security management process. This led us to conduct **study 5**[23]**,** which involved using one of the five organisations as a test-bed for development and making suggestions concerning the steps needed to bridge the perception gap between the general management and technicians when addressing the ICT security management problem in the organisation.

Finally, and which brought us back to the original problem, following the practical observations in the field and the experience gained in the five studies[24], and based on the systems theory and other existing ICT security management approaches, a new holistic approach for managing ICT security in non-commercial organisations was proposed. More detailed discussion of these observations and the justifications for the need of the new approach are presented in section 3.6, and the proposed holistic approach which is the second main contribution of this thesis is presented in chapter 4. Examples of a practical experience in implementing some of the components of the proposed approach are presented in Paper VI and VII.

ICT Security Awareness Seminars

During this research process and our fieldwork in Tanzania, a number of public seminars were conducted. These included nine ICT security seminars and public lectures which took place, with more than 1,000 participants at the following places: Tanzania Commission for Science and Technology (COSTECH) on 13th July, 2004; later in November 2004, at the University of Dar es Salaam (UDSM); State University of Zanzibar; University College of Land and Architectural Studies (UCLAS) and Institute of Accountancy Arusha (IAA). In addition, a seminar for decision-makers was successfully conducted at the Royal Palm Hotel in Dar es Salaam. This seminar attracted CEOs, IT directors and senior Government officials. Another session was the one to which the author was invited as a guest speaker to talk about "ICT Security Management, A holistic approach" at the Information Security and Audit Workshop organised by ISACA, Tanzania Chapter at the Golden Tulip Hotel on August 23, 2006. This was during the launch of the ISACA Tanzania chapter where participants included Chief Executive Officers, Directors of Finance and Administration, IT Professionals, Internal and External Auditors, Investigation Officers, ICT Security Professionals and people from the National Board of Accountants and Auditors (NBAA) Tanzania. Furthermore, additional seminars with the Tanzania Police Force

[23] See study 5 and Paper VI
[24] See the summary of papers resulted from the five studies in chapter 5

at Tanzania Global Development Learning Centre and other sessions (seminars and meetings) were conducted in the five organisations under study. Some of the sessions were feedback from the preliminary findings in their respective organisations, as well as the individual sessions during the fieldwork in the five organisations. These seminars gave us feedback which was useful during the research process.

1.7 Publications

This thesis includes seven publications listed in order of their contribution to the research questions. For each listed publication, a research question which is addressed by the publication is pointed out, together with the author's individual contribution.

PAPER I: Bakari, J. K., Tarimo, C. N., Yngström, L., & Magnusson, C. (2005) *State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case study*. Proceedings of the 5th IEEE International Conference on Advanced Learning Technologies" (ICALT 2005) in Kaohsiung, Taiwan July 5 - 8, 2005, pp. 1007-1011, ISBN 0-7695-2338-2. Main Author
Addresses research Question: Res.Q.1

PAPER II: Bakari, J. K., Magnusson, C., Tarimo, C. N., & Yngström, L. (2005) *The Mitigation of ICT Risks Using EMITL Tool: An Empirical Study*. Proceedings of the International Federation for Information Processing (IFIP) Volume 193, TC-11 WG 11.1 & WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems, **eds.** Dowland, P., Furnell, S., Thuraisingham, B., Wang, X., (*Springer*) pp. 157-173, Fairfax, Virginia, Washington, USA, December 1 - 2, 2005, ISBN: 0-387-29826-6. Main Author
Addresses research Question: Res.Q.2

PAPER III: Bakari, J. K., Magnusson, C., Tarimo, C. N., C. Yngström, L. (2006) *Outsourcing ICT security to MSSP: Issues and Challenges for the developing world.* Proceedings of Information Security South Africa (ISSA), from insight to foresight Conference, **eds.** Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM, Sandton, Johannesburg, South Africa, July 05-07, 2006, ISBN: 1-86854-636-5. Main Author
Addresses research Question: Res.Q.2 and Res.Q.3

PAPER IV: Bakari, J. K., Tarimo, C. N., Mutagahywa, B. (2006) *Issues and Challenges to be addressed in e-Government from an Information Security Point of View*. Proceedings of the IST-Africa 2006 International Conference, Pretoria, South Africa. 03-05 May, 2006, Paul Cunningham and Miriam Cunningham (**Eds**). IIMC International Information Management Corporation, ISBN: 1-905824-01-7. Main Author
Addresses research Question: Res.Q.3

PAPER V: Tarimo, C. N., **Bakari, J. K.**, C. Yngström, L., Kowalski, S. (2006) *A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards A Culture of ICT Security – The Case of Tanzania.* Proceedings of Information Security South Africa (ISSA), from insight to foresight Conference, **eds.** Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM, Sandton, Johannesburg, South Africa, July 05-07, 2006, ISBN: 1-86854-636-5. Co-Author
Addresses research Question: Res. Q. 4

PAPER VI: Bakari, J. K., Tarimo, C. N., & Yngström, L., Magnusson, C. & Stewart Kowalski, *Bridging the gap between general management and technicians – a case study on ICT security in a Developing Country"* Journal of the International Federation for information Processing (IFIP), Computer & Security, The International Source of Innovation for the Information Security and IT Audit Professional, *ELSEVIER* Vol. 26/1 pp 44-55. Main Author.
Addresses research Question: Res.Q.5

PAPER VII: Bakari, J. K., Magnusson, C., Yngström, L., Tarimo, C. N. (2007) *Operationalisation of ICT Security Policy, Services and Mechanisms in an organisation.* Proceedings of the IST-Africa 2007 International Conference, to be held at Joaquim Chissano International Conference Centre, Maputo, 09 – 11 May 2007. (Forthcoming), Main Author.
Addresses research Question: Res.Q.5

The following publications which are either covered in part I – Prologue or updated to journal are not included in the thesis.

PAPER VIII: Bakari, J. K., C. Yngström, L., Magnusson, C., Chaula, J., *Towards Managing ICT Security in Non-Commercial Organisations in Developing Countries,* Proceedings of Information Security South Africa (ISSA), enabling tomorrow Conference, **eds.** Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM, Midrand, Johannesburg, South Africa, June 30 - July 02, 2004. Main Author
Addresses research Question: Main Research Question

PAPER IX: Bakari, J. K., Tarimo, C. N., & Magnusson, C. Yngström, L., *Bridging the gap between general management and technicians – a case study in ICT security,* Proceedings of the International Federation for information Processing (IFIP), Volume 201, Security and Privacy in Dynamic Environment, **eds**. Fischer-Hubner, S., Rannenberg, K., Yngström, L., Lindskog, S. (*Boston: Springer*), pp. 442 – 447, Karlstad, Sweden, 22-24, May 2006, ISBN: 0-387-33405-X **(Updated to Journal),** Main Author
Addresses research Question: Res.Q.5

1.8 Structure of the thesis

This thesis is divided into three main parts, namely Prologue, Publications, and Appendices. The Prologue presents the introduction (chapter 1), research methodology (chapter 2), theoretical foundation for ICT security and management (chapter 3), and the proposed holistic approach for managing ICT security in non-commercial organisations (chapter 4). We have also included in the prologue section (chapter 5), a summary of each of the appended papers to briefly give the reader who does not have enough time to go through them an idea of what the paper is all about. Concluding remarks and suggestions for further work are presented in chapter 6.

Chapter 2

2. Research Methodology

2.1 Introduction

In this section the research strategy and methodologies adopted in our work are investigated. Given the multi-disciplinary nature of the problem, investigation into what exists in practice and suggesting the remedy was the way forward. This was made possible through a number of studies based on different research strategies and methodologies.

One of the common ways of doing research is using quantitative and qualitative research methods. Quantitative research is the systematic scientific investigation of quantitative properties, phenomena and their relationships by classifying features, counting them, and constructing statistical models in an attempt to explain what is observed. Examples of quantitative methods include survey methods and laboratory experiments. According to Creswell (1998), qualitative research is a study conducted in a natural setting where the researcher, an instrument of data collection, builds a complex holistic picture, gathers words or pictures, analyses them inductively, focuses on the meaning of participants, and describes a process that is expressive in language. Examples of qualitative methods are action research, case study research and ethnography. Qualitative data sources include observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and reactions (Myers, 1997; 1999).

2.2 Research Strategies

With reference to Myers (1999) and Bjorck (2005), because of the nature of the problem[25] we have, it can best be studied using research strategies such as survey, action research and case study which are mainly qualitative.

(a) **Survey research:** The survey research is a comprehensive system for collecting information that involves one or a combination of two procedure(s): questionnaires; and interviews. A questionnaire is almost always self-administered, allowing respondents to fill them out themselves. The researcher is responsible for delivery and collection of the questionnaire. An interview typically occurs whenever a researcher and respondent meet face-to-face or communicate through some type of medium such as telephone or computer. There are three sub-types of interviews: unstructured, which allows unstructured communication in the course of the interview or questionnaire administration; structured, where the

[25] See section 1.2 and 1.5

researcher is highly restricted on what can be said; and semi-structured, which restricts certain kinds of communication but allows freedom of discussion of certain topics(O'Connor, 2004). In our work both questionnaires and interviews were used in a semi-structured way.

(b) **Action Research:** According to Rapoport,
"Action research can be described as research that aims at contributing to the practical concerns of people in an immediate problematic situation"
(Rapoport, 1970, pp. 499).

It is also supported by Robert (2003) that action-oriented research enables the researcher to investigate a specific problem that exists in practice. Robert argues that the researcher should be involved in the actions that take place.

Action research is characterised by the following features:

- *Problem-aimed research focuses on a special situation in practice. Seen in a research context, action research is aimed at a specific problem recognisable in practice, where the outcome of the problem solving is immediately applicable in practice.*
- *Collective participation, where all participants (e.g. the researchers and persons standing in the practice) form an integral part of action research with the exclusive aim of assisting in solving the identified problem.*
- *Type of empirical research, which is characterised by a change in practice while the research is going on.*

(Gerber, 2003)

(c) **Case Study Research:** According to Robert Yin (1981; 1994) in (Robson, 2002), case study is a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context. Case study is used in our study to mean two things. First it is used to describe a unit of analysis[26] and secondly to describe a research method to study a phenomenon in its real setting and environment. According to Yin (1994), a case study is a useful research method when it is difficult to isolate the phenomenon from its environment. In our work the focus is on ICT security management in organisations where the interest has shifted to organisational rather than technical issues as also suggested by Myers (1999). The downside of case study includes the time it consumes and its labour-intensive requirements. In our study we coped with this disadvantage by limiting the size of the study to five organisations and selected respondents as detailed in the section 2.3 "research design".

Referring to the research questions, and depending on the nature of the study, different methods have been applied to different studies as detailed in section 2.3.6.

Figure 2-1 summarises the research strategies used in all five studies and the underlying philosophical assumptions of the entire study (all five studies). The methods presented in the solid boxes are the ones used in our research, using mainly the qualitative approach.

[26] Tanzania and in particular the five non-commercial organisations

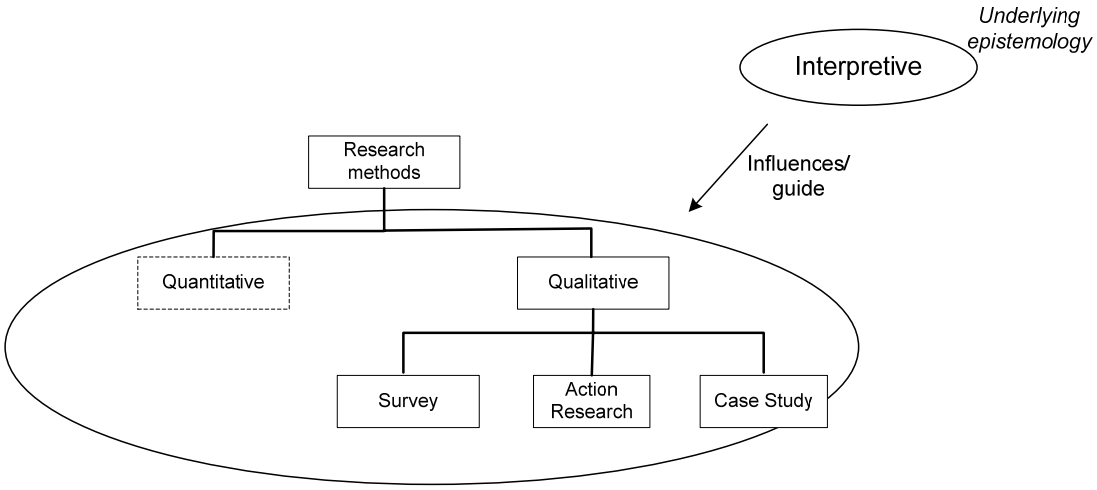


Figure 2-1: Research Strategies & Underlying Philosophical assumptions

2.3 Research Design

The entire research is guided mainly by interpretive epistemology as a philosophical assumption. Epistemology refers to the assumptions about knowledge and how it can be obtained. In this study we assume that the management of information and communication technology in organisations could be explored from the frame of reference of those who are directly involved in the process (Bjorck, 2005). Therefore, as suggested by Davison (1998), this research can be classified as *interpretive.*

> *Interpretivists contend that only through the subjective interpretation of and intervention in reality can that reality be fully understood. The study of phenomena in their natural environment is key to the interpretivist philosophy, together with the acknowledgement that scientists cannot avoid affecting those phenomena they study. They admit that there may be many interpretations of reality, but maintain that these interpretations are in themselves a part of the scientific knowledge they are pursuing.* (Davison, 1998, pp. 32)

We have selected interpretive epistemology as our main philosophical assumption of the study because of the nature of the problem[27] we have in hand, and hence the nature of the research. This philosophical assumption requires a study "the management of ICT security in the organisations" to be conducted in its natural environment, as supported by Myers (1999) and Bjorck (2005).

In order to have better understanding of the problem, the decision was made to select five non-commercial organisations for the case study. Non-commercial organisations as used in this work are those organisations whose main objectives are not to make profit but to provide a service to the public. As pointed out in the introduction, the selection of the non-commercial sector was because it would be feasible to get the required information during the research since most of these are government organisations and they are public. Given the nature of the research question and the proposed approach it required having more than one organisation to be studied. On

[27] See the main research question

the other hand, in order to get more detailed results it was not feasible to conduct it in many organisations. This was found to be due to time and resource constraints and so the balance of 5 organisations was reached. Among the non-commercial organisations, we were greatly motivated to conduct our study mostly in institutions of higher learning because it would be even more feasible to be able to collect the information we were looking for in our research. However, in order to reach our research objectives, we also had to have other non-commercial organisations which are not higher learning institutions. The selection method for the three academic institutions was based on the following criteria and reasons: first they are the largest in their area of specialisation or focus in the country; secondly, the problem being researched was first observed in the area (the researcher has been working for more than six years in one of the institutes); thirdly there are other ongoing researches in the area but in a different direction, not focusing on the management of ICT security. At some stages the selection involved local ICT experts and the experts from the security lab at DSV. A similar method was used to identify the two remaining non-commercial organisations, which are also the largest in their area of specialisation or focus in the country and owned by the government. By virtue of being non-commercial organisations, the way they deploy, use, secure and manage ICT in general and ICT security in particular gives a fair representation of the state of ICT security management in other organisations of a similar set-up in the country. There was no reason for mentioning the names of the studied organisations. Our interest was to study the state of ICT security management and so the studied organisations are referred to as **X**, **Y**, **Z**, **U** and **V** throughout our discussion. In this case, our level of analysis is organisational.

The data-gathering instruments employed were questionnaires with multiple choice and open-ended questions, and face-to-face interviews with some selected respondents. Also, onsite observation (participatory) and documentary review was used. The respondents were mainly Chief Executive Officers (CEOs[28]) (n=5), Chief Financial Officers (n=5), Operational managers (n=20), IT Managers and systems administrators (n=22) and general and technical staff (n=16). Table 2-1 shows the respondents' distribution. The details of the interview guides are presented in Appendix (A-1, A-2, B, C, D and E).

Table 2-1: Summary Respondents distribution

Organisation	**X**	**Y**	**Z**	**U**	**V**	**Total**
Top management (CEOs)	1	1	1	1	1	5
Financial Officers (CFOs)	1	1	1	1	1	5
Operational Management	5	3	5	5	2	20
Operational manag. in IT Dept	9	8	2	2	1	22
General and Technical staff	3	5	3	2	3	16
Total	**19**	**18**	**12**	**11**	**8**	**68**

Source: Research findings

2.3.1 The studied organisations

In this section we briefly describe the five organisations identified for study in Tanzania.

[28] Used in this study to mean people in the top senior position

2.3.1.1 Organisation X

Organisation **X** is a higher learning institute with approximately 1,700 staff (academic and administrative) and a student population of approximately 14,000 (undergraduate and postgraduate). The utilisation of ICT at organisation **X** can be traced back to 1995, when the ICT strategic plan was put in place for the first time. The organisation has more than 2,000 personal computers (PCs), with probably the best network infrastructure in the country. There are three main core services, the substantial number of functions of which have been and still are in the process of being computerised. The majority of the information systems (databases) in the organisation which handle thousands of records are not integrated. This means, these information systems handle services independently of each other although most of the subjects (customers) are the same. The amount of data being exchanged in the network locally is not very high as compared with the international traffic which is always beyond 98% of bandwidth utilisation during the peak hour for 1.5 Mbps link.

2.3.1.2 Organisation Y

Organisation **Y** is a government-based service provider operating in 21 regions[29] throughout the country. The organisation had 1,300 staff in the past, which it downsized to 900 in 2003 and it is still working on reducing the number to 600 in the near future. There are four main core services. Each provided service is to some extent dependent on ICT to meet its objectives. The information systems that run the core services of the organisation are centralised. This means that data are collected from different branches by various means and brought to the head office for processing. The organisation has approximately 2 million customers scattered throughout the country, 25% of whom are active. The organisation is now in the process of migrating from working in a closed environment to inter-operable platforms with TCP/IP as the foundation and with the mission of putting their services online. There are approximately 400 PCs for the entire organisation. Only the head office and four branches are connected to the internet, mainly for communication purposes.

2.3.1.3 Organisation Z

Organisation **Z** conducts its operations, mainly distance learning, through regional and study centres. Currently there are 23 regional centres and 69 study centres throughout the country, with approximately 371 academic and administrative staff and a student population of more than 16,000. The organisation has approximately 112 PCs with 71 PCs networked in a small LAN at its head office. A very small part of the organisation's core services is computerised. There are only two information systems operating independently in the form of a database but handling thousands of customers.

[29] Tanzania is divided into 26 regions

2.3.1.4 Organisation U

Organisation **U** is a government-based service provider operating in all the major regions. The organisation has approximately 800 staff. There are three main core services and each is to some extent dependent on ICT in meeting its objectives. The organisation is now in the process of building a backbone infrastructure to interconnect its departments and to improve the service to its tenants. There are approximately 140 PCs for the entire organisation. Currently, due to the absence of a backbone infrastructure, the information systems are not integrated. Currently, the organisation has small isolated LANs that exist in various departments and at the head office. For the same reason, the information systems are also isolated. The organisation manages more than 120 tenants, most of them being small organisations, most of which have their own LANs with independent internet connections.

2.3.1.5 Organisation V

Organisation **V** is a higher learning institute with approximately 300 academic and administrative staff and a student population of 1,200. The organisation has a backbone infrastructure made up of fibre optic double rings and wireless, which has about 32 access points as back-up. Each department has a LAN, which is reachable from other departments and internet through the physical cable and wireless. There are approximately 200 PCs of which 80% are connected to the organisation's network. We learned also during the survey that approximately 200 more PCs will be added in about three months' time[30].

2.3.2 Data collection

Depending on the study (1-5) in hand, the discussion, the data involved and the methods differ from one study to another. However, the main source of data was the same and the data collection methods used were questionnaires, participation, direct observations and documentary review as detailed below.

The research activities started during the spring of 2003 with a literature review of the theoretical background in ICT security management. We then perused the current state of ICT security problems globally and the situation in the developing countries with more attention paid to Tanzania. Initially this was done through documentary review and direct observations. The secondary data which were obtained from libraries provided a general background to ICT and ICT security in the developing world and Tanzania in particular. Later, we went through various existing frameworks, standards and best practices in ICT security management such as ISO 17799, OCTAVE, COBIT and ITIL. In addition, a more thorough study of the BRITS framework (its processes and customisation for application to a non-commercial organisation) also took place.

[30] From the time the survey way conducted

2.3.3 Pre-test

Between March and May 2004, we adopted a questionnaire from the OCTAVE method by (Alberts & Dorofee, 2003, pp 363). Since our first goal was to assess the current state of ICT security and to uncover the likely problems and potential consequences arising from ICT risks, the questionnaire presented in (Alberts & Dorofee, 2003) seemed to cover most of our requirements. Another important aspect was to work out the basis for BRITS framework implementation. These two reasons made us decide to adopt questions from the OCTAVE method and customise them for the developing countries, in this case Tanzania (the environment where the study was going to take place). The first draft was presented to ICT security specialists (research students coming from developing countries) and also to ICT security experts within the ICT security research lab at the Department of Computer and Systems Sciences (DSV) at Stockholm University for comment. The refined draft was then presented to four ICT experts and two ICT specialists in Tanzania between June and July 2004 for their comments. After minor refinements, eight questionnaires were distributed for testing purposes to eight respondents in the first half of August 2004.

The results were used to further fine-tune and customise the questionnaires. Finally, we had the 4 questionnaires for different personnel with the number of questions indicated in brackets; General staff and technicians (22), Senior Management (27), Operational Management (28) and Technical staff (68). This process we referred to as the first customisation and validation process is shown in Figure 2-2.

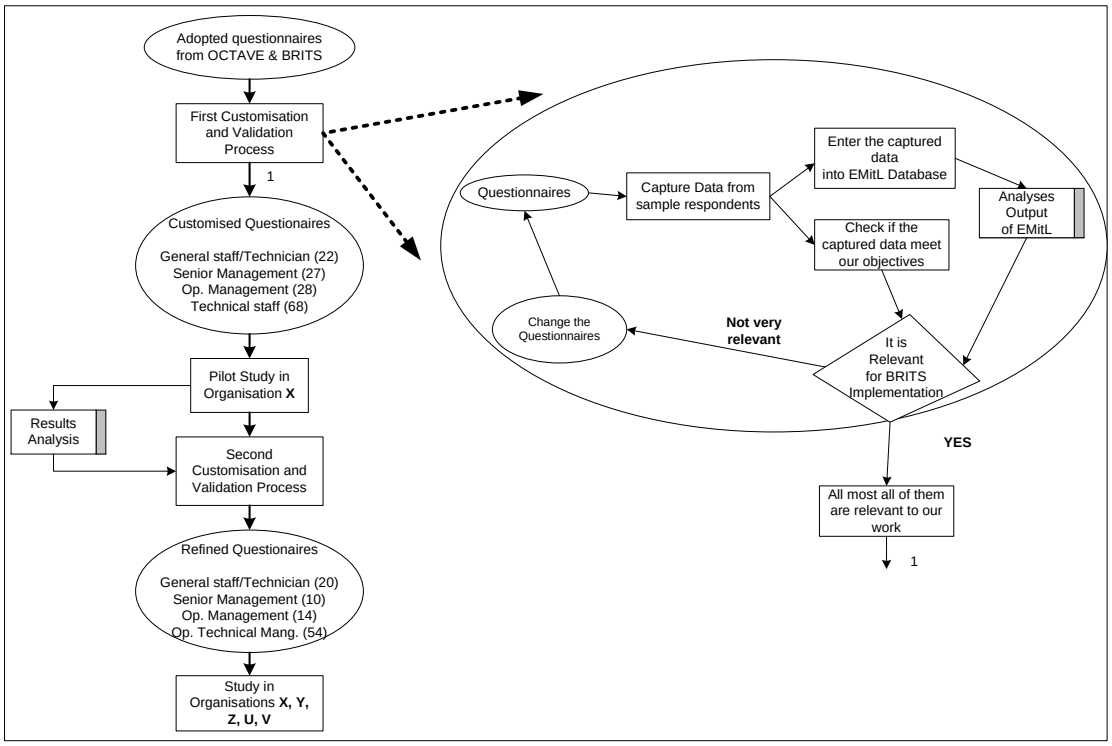


Figure 2-2: Development of the study questionnaires

2.3.4 Pilot study

A pilot study was later conducted between mid-August and October 2004, where 80 questionnaires were distributed to 80 respondents in organisation **X.** The selection of the respondents was based on the organisation's structure and within the group a random selection method was used to select the respondents. During this stage we defined the senior or top management as the CEOs and the directors. The operational management involved the heads of department/units. The operational/technical management involved the system administrators and IT managers of various departments, and the last group were ICT technicians and ICT users like data entry staff. A total of 56 respondents returned the filled-in questionnaires as indicated in brackets in Table 2-2.

The results of the pilot study indicated that the subject of ICT security was new to many respondents. This was indicated by the fact that many questions were either answered with **don't know** or left **blank**. For interpretation purposes, **don't know** could mean don't understand the question OR don't know if the practice exists or not. There were even some comments like "This is too demanding!!! …". Although some respondents acknowledged that the questionnaire itself with the introduction was very educative, you would find a comment like this: "We never knew this … we would like to see the results of the work …" Of the final figure of 56, during the study only approximately 20 respondents returned their questionnaires on time, meaning after a period of 2 to 3 weeks. The majority misplaced the questionnaire several times and there are cases where it took the whole 3 months to follow up one respondent who every time had to be provided with a new copy of the questionnaire. On the other hand, everyone had the intention of filling in the questionnaire, but the problem was time, as they claimed that they were busy with other responsibilities[31].

2.3.5 Study at the five organisations

Based on the pilot study results, we further fine-tuned the questionnaire between November and December with the help of visiting Professors to Tanzania from the Department of Computer and System Sciences, Security lab. From December 2004 to February 2005, we conducted face-to-face interviews with selected respondents, mainly the CEOs, chief financial officers, operational managers, IT directors and managers, system administrators and general staff and technicians. This time the method used was to book an appointment of between 20-30 minutes, although it only worked with the CEOs. For the rest of the respondents, we had to visit them in their offices at short notice as they become available. In practice most of the sessions lasted between 30 and 60 minutes, with some lasting for more than 1 hour. The final version of the questionnaires were prepared as follows: the first was addressed to the top management with 10 questions at strategic level; the second to the operational management with 14 operational level questions; the third to the technical department with 54 questions covering operational procedures and implementation issues – mostly about technical countermeasures; and the fourth one to general staff with 20 questions on implementation and practice. The letters of introduction both to the

[31] I must admit that a number of senior and operational staff were indeed extremely busy, more than busy actually in my opinion! There were many responsibilities assigned to them, mainly due to shortage of staff. For example, one senior staff member had four different offices, all handling urgent matters of the organisation!

organisation and respondents and the questionnaires used during the interview for all four groups are found in Appendices A to E. About 88.3%[32] of the potential sampled respondents identified from the organisational structures were successfully interviewed. Table 2-2 summarises the distribution of the respondents by categories and surveyed organisations, and Table 2-3 shows the distribution of the total number of staff, potential respondents depending on the organisational structure and the interviewed respondents for each organisation.

Table 2-2: Respondents' distribution including pilot study

Organisation	**X**	**Y**	**Z**	**U**	**V**
Top management (CEOs)	1*(8)	1	1	1	1
Financial Officers (CFOs)	1(1)	1	1	1*	1
Operational Management	5(20)	3	5	5	2
Operational manag. in IT Dept	9(14)	8	2	2	1
General and Technical staff	3(13)	5	3	2	3
Total	**19 (56)**	**18**	**12**	**11**	**8**

Source: Research findings

Note:

- * Representative or Acting in the position
- Numbers in the brackets (first column) are from the pilot study in organisation X
- During the pilot study at organisation **X**, we distributed 80 questionnaires and 56 respondents returned them.

Table 2-3: Selection of respondents in each organisation

	Organisation	**Total Number of Staff in the organisation**	**Potential respondents (from the organisational structure)**	**Interviewed respondents**
1	**X**	1700	25	19
2	**Y**	900	18	18
3	**Z**	371	14	12
4	**U**	800	12	11
5	**V**	300	8	8
	Total	**4071**	**77**	**68**

Source: Research findings

The selection of the respondents was based on the organisational structure and allocation of core services in a particular organisation. We use core services in our work to refer to the main services that the organisation is responsible for or entitled to offer, consequently enabling it to achieve the objective of its existence.

As stated earlier, the face-to-face interview was used to gather the information. Much time was spent in the five organisations to make participatory observations and where necessary verify the collected information by going through various referenced[33] documents.

[32] 68 successfully interviewed out of 77 potential respondents
[33] Documents referenced by the respondents during the interview

Except for organisation **X**, the interview in all the other organisations started with the CEO. In that case, it was possible to get a good overview of the organisation's structure and how the core services are located within the organisation. There was an opportunity to observe and verify or follow up for clarification anything that was not clear to the respondents.

2.3.6 Research methods applied to the five studies

In section 1.6 we briefly described how the research evolved from start to finish through the different studies[34]. In the following section we explore in detail how the discussed methods in the sections above were used in each study and the reason why a certain method was selected and used in a particular study.

(1) Study 1: This study had two primary goals: firstly to assess the current state of ICT security management, mainly with respect to ICT security strategies, policies and their implementation, as well as operational issues. Secondly, to uncover the likely problems and potential consequences due to ICT risks as the dependency of organisations' core services on ICT grows. To achieve these two goals, we used *survey* and *case study* methods, because we needed to collect data in the three organisations (X, Z, & V). Questionnaires, face-to-face interviews, observations and documentary review were used to guide the study as detailed in section 2.3.5 above.

(2) Study 2: The goal of this study was to investigate the prerequisites for utilising the existing solutions (using EMitL[35] tool, and outsourcing the management of ICT security to a third-part organisation called MSSP[36]) in addressing the observed state of the ICT security problem. To achieve this goal, similar *survey* and *case study* methods have been used in this study to gather and analyse data from the five organisations (X, Y, Z, U and V).

(3) Study 3: The goal of this study was to discuss the issues and challenges to be addressed in the initial stages of computerisation. To achieve this goal, a *case study* of e-government systems was undertaken. Reports of various government projects in developing countries were reviewed, and used together with secondary data sources from the literature to guide the study.

(4) Study 4: The goal of this study was to investigate the important aspects to be taken into consideration in order to successfully manage ICT security. Security in ICT touches upon many issues, both social and technical in nature. The issues can be such as security knowledge of the users, which in turn touches upon the educational system of Tanzania and the general security culture of the country in question—where the studied organisations are located. Using the *survey* method, six training institutes offering ICT training and education in the country were

[34] See figure 1-6 for quick reference
[35] Estimated Maximum information Technology Loss
[36] Managed Security Services Provider

involved, their training and educational materials and programmes being scrutinized for aspects of ICT security content. A criterion for selection was to include institutes with training and/or educational programmes in ICT. The prime target was on institutes whose programmes are exclusively geared towards ICT training and/or education. These were complemented by other institutes whose curricula include ICT studies in parallel with other fields. At the national level, strategies and policy documents regarding education and training were obtained for reviewing. The collected data were then analysed to show some trends or patterns, which were then compared with some well known examples of good practice in fostering security culture. The primary data sources were, in addition, complemented by secondary data sources from the literature.

(5) Study 5: The goal of this study was to investigate how the ICT security management process could be improved in a non-commercial organisation. This was achieved through conducting *action-research* conducted using organisation Y. Organisation Y was selected as a test-bed for experiment from August 2005 through to August 2006, during which time the *case study* was conducted. Organisation Y was selected as a test-bed for the following reasons. First, the organisation was in the process of migrating from proprietary systems to open, inter-operable platforms with TCP/IP as the foundation. In the process of migration, the organisation was planning to implement nine information systems which involved migration from a closed ICT environment (operating in a sort of island – where all data were collected from different branches located in different regions and processed centrally) to a new, open, inter-operable system, together with the organisation's mission to have the services available via the internet. This increased the organisation's exposure to ICT-related risks. Hence there was an immediate need to improve the management of ICT security in the organisation. Secondly, and most important, was the willingness of the management to incorporate into the main project the security sub-project of which the author—researcher was appointed as the team leader.

Table 2-4 summarises the research methods used for each study, in which, a specific research method/s was used within the research strategies above.

Table 2-4: Summary of the research methods used

Study/Research Questions	Research Methods			
	Qualitative	Case study	Survey	Action
1	√	√	√	
2	√	√	√	
3	√	√		
4	√		√	
5	√	√		√

Chapter 3

3. Theoretical foundation for ICT Security Management

In chapter 2 we discussed the strategies and how we approached the problem using various studies. In this chapter, the theoretical foundation for ICT security management is presented.

3.1 Introduction

ICT Security Management is the overall process of establishing adequate ICT security within an organisation in order to achieve and maintain appropriate levels of confidentiality, integrity and availability of information and services. Caralli (2004) describe managing security as planning, organising, commanding, coordinating, and controlling it for the benefit of all stakeholders. ICT security management involves a complete range of administrative, procedural and technical measures needed to fulfil an organisation's security objectives (Caelli et al., 1991). Eloff et al. (2003) and Bishop (2003) describe ICT security management as a combination of several aspects involving policies, standards, guidelines, codes-of-practice, technological, human, legal and ethical issues. It is also argued that ICT security is not only about products and standards, but also the effective management of processes between policies, procedures, technologies and supporting structures along with the environment where it is being implemented (Eloff et al., 2003). Various literatures indicate that the nature of the ICT security management problem is a multi-disciplinary one and requires a systemic-holistic approach (Kowalski, 1994; Yngström, 1996; Magnusson, 1999; Frisinger, 2001; Eloff et al., 2003). In view of these claims, in the next section we explore the holistic approach concept and its origin—the systems theory - first. We then look at the ICT security management process and the existing ICT security management approaches.

3.2 The systems theory and Holistic Approach

We shall in this section discuss a few concepts concerning General Systems Theory (GST) as a basis for the holistic approach and hence the foundation for our work.

"Modern technology and society have became so complex that traditional ways and means are not sufficient any more but approaches of a holistic or systems, generalist or inter-disciplinary nature become necessary" (Bertalanffy, 1972, pp 420).

The quote above from Von Bertalanffy (1972) is in agreement with the previous section's claims, which calls for a holistic approach if we are to address the ICT

security management problem. Von Bertalanffy argued for the concept of ‘system’. He used ‘system’ as an epistemological (abstraction) device to describe organisms as wholes, and showed that it could be generalised and applied to wholes of any kind.

Definition

> *"System is a set of objects together with relationships between the objects and between their attributes related to each other and to their environment so as to form a whole."*
>
> (Schoderbek et al. 1990 pp. 13)

Systems are made up of sub-systems, which are further made up of sub-sub-systems, with the following characteristics as proposed by Churchman (1968) in (Schoderbek et al. 1990 pp. 9-13).

1. **Objectives of the total system together with performance measures:** The objectives of the system refer to those goals or ends toward which the system tends;
2. **The system’s environment:** Refers to the environment as lying outside the system’s control, which in part determines how the system may perform. The environment is beyond the system’s control;
3. **The resources of the system:** refers to all resources available to the system for the execution of the activities necessary for goal realisation,
4. **The components of the system:** refers to all those “activities” or “mission” or “jobs” that contribute to the realisation of the system’s objectives; and
5. **The management of the system:** this refers to the need for planning and controlling the system. Connected with the planning and control function of the system is the notion of information flow or feedback, the characteristics of cybernetic systems. According to Churchman, without sufficient feedback, the planning and control functions would be inadequate.

A system can be closed or open. A system is considered closed if no materials enter or leave it and it is open if there is inflow and outflow, and therefore a change of the component material (Bertalanffy, 1950; 1968). Of particular interest to our work and hence involving more discussion is the open system concept as shown in figure 3-1. In the figure *input*, can be an output from another system or a feedback from the system itself, *process* is the transformation of inputs to outputs, and *output* consists of consumables by other systems, consumables by the system in the next cycle, and wastes. It is argued that a system cannot control its environment, but on the contrary, is dependent on or controlled by the environment. However, the system may influence its environment through its output (Schoderbek et al. 1990).

.

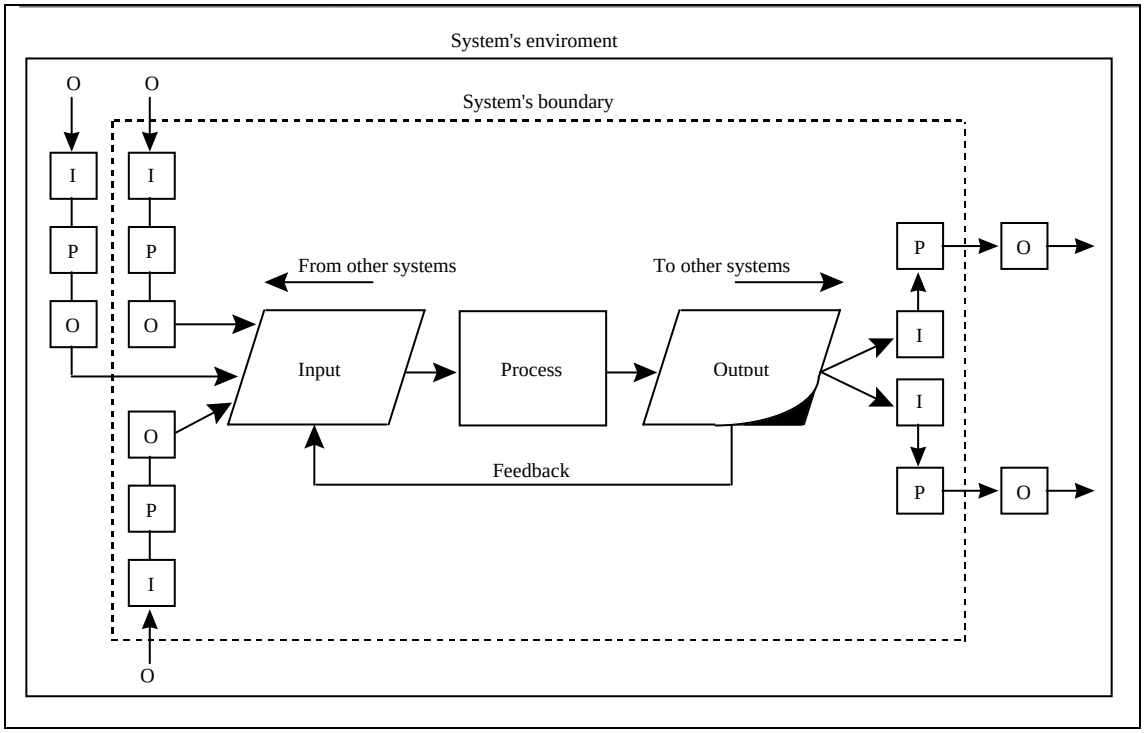


Figure 3-1: An open system (Schoderbek et al. 1990, pp. 25)

Notes: I – Input
P – Process
O – Output

Furthermore, we found the following fundamental hallmarks of the General Systems Theory as presented by Schoderbek et al (1990, pp. 38) and further explained from a security point of view by Yngström (1996, pp. 36), a very useful and thought-provoking tool when extending and developing the new knowledge from the series of studies we conducted and the few concepts introduced above.

The 10 hallmarks are:

1. **In all systems there exist interrelationship and interdependence of objects and their attributes:** This shows that unrelated and independent elements can never constitute a system. It also facilitates delimiting the system from its environment, and analysing important chains of relations and dependencies.

2. **Holism:** All systems have a wholeness that cannot be found through breaking up the system into parts. The systems approach is not an analytical one, where the whole is broken down into its constituent parts, and then each of the decomposed elements is studied in isolation; rather, it is a wholeness type of approach, attempting to view the whole with all its interrelated and interdependent parts in interaction. For example, it is not enough to implement a “top-of-the-range firewall” and believe that it will function as intended.

3. **Goal seeking:** All systems are goal seeking. The ideas behind ICT security management is to deduce, find, and specify security goals from the goals of the organisation or business, establish measurable security objectives, establish strategies to achieve these objectives, and establish efficient controls of these goals using feedback in the system. In the same way, for ICT security management to be successful, it must be aligned with the business and hence the organisation’s goals.

4. **Inputs and Outputs:** All systems are dependent on some inputs that, when transformed into outputs, will enable the system to reach its ultimate goal. All systems produce some outputs needed for other systems. Wrong, false, or untimely inflow can disturb the production and therefore result in inefficient or false outflow.

5. **Transformation Process:** All systems are transformers of inputs into outputs. This is the only way to attain their goals.

6. **Entropy:** All systems have a degree of structural order or disorder - entropy. Open systems can compensate disorder by adding extra matter, energy and/or information. This way the system is controlled, which is really the aim of the security system as suggested by Yngström (1996).

7. **Regulation:** All systems need to be managed (regulated) in some fashion so that the system's goals can ultimately be reached. Management implies planning and controlling by feeding back information in order to check that plans are being followed. Feedback is a requisite of effective control.

8. **Hierarchy:** Systems are generally complex wholes made up of smaller sub-systems. The nesting of systems within other systems is what is implied by hierarchy, which means that systems comprise sub-systems, which in turn comprise sub-sub-systems, and so on. The structure of a system is essential for its management and control – more complex ones (with many interacting components) are very difficult to control and thus to make secure.
   Schoderbek et al. (1985) extended this concept into the following propositions:
   (a) A system is always made up of other systems
   (b) Given a certain system, another system can always be found that comprises it, except for the Universal System, which comprises all others.
   (c) Given two systems, the one system comprising the other can be called the high-level system in relation to the system it comprises, which is called the low-level system.
   (d) A hierarchy of systems exists whereby lower-level systems are incorporated into high-level systems.
   (e) The low-level systems are in turn made up of other systems and can, therefore, be considered the high-level system for the lower-level systems to be found in it.

9. **Specialisation:** In complex systems, specialised units perform specialised functions. In this way the total system can adapt more quickly and thereby more efficiently and effectively to changes in the environment or within the system itself. ICT security management and operation need to be in such a specialised unit.

10. **Equifinality:** Open systems can reach their goals in many different and valid ways. They are not constrained by the simple cause-and-effect relationships found in physical systems, but can attain their objectives with varying inputs and transformational processes.

The 10 hallmarks make a good and simple checklist and facilitate the understanding of the overall picture of ICT security management in an organisation.

In addition to the ten hallmarks, we also found the following two main concepts useful when dealing with the ICT security management problem.

Firstly is the system's holistic principle:

"A system has holistic properties not manifested by any of its parts. The parts have properties not manifested by the system as a whole" (Skyttner, 2001)

In other word as argued in the 10 hallmarks, a system as a whole works differently from the parts of the system. The parts alone cannot do what the system can and, therefore, it is necessary for a system to have expert functional parts that communicate efficiently.

Secondly, the Complementary Law:

*"Any two different perspectives (or models) of a system will reveal truths regarding that system that are neither entirely independent nor entirely compatible" (*Weinberg 1975)

Consider four senior staff coming from different departments, namely technical, legal, human resource and internal audit, looking at the security problem: the first perceives it to be a technical problem, the second a legal problem, the third regards the human aspect of the problem and the fourth looks at the problem as part of risks to the business. Separately, each of them would paint a different picture from the others based on each one's partial experience. Yet, when they put the four pictures together, they would build a better and truer picture—the ICT security problem.

Based on General System Theory, Yngström (1996) proposed the systemic-holistic model (see figure 3-2) that helps individuals to understand security problems as related to originally existing physical entities on specific abstract levels in specific contexts. The model is organised into three dimensions; level of abstraction, context orientation and subject area.

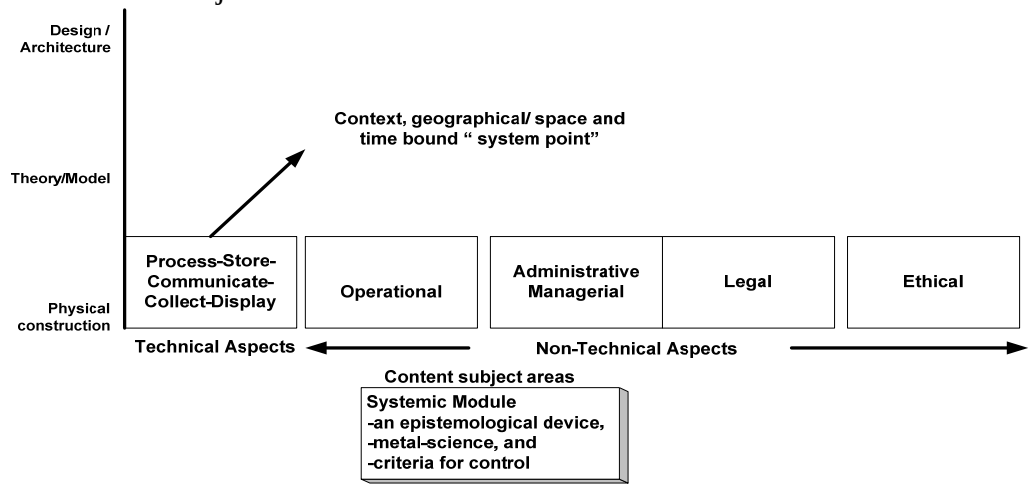


Figure 3-2: The systemic-Holistic Model (Yngstrom, 1996, pp. 20)

According to Yngström (1996), the Systemic Module may be viewed as the theory of knowledge, especially the critical study of its validity, methods, and scope. It can also be viewed as a meta[37] science but most important is that it states criteria for control. The content of the Systemic Module is based on General Systems Theory, Cybernetics[38] and General Living Systems.

"Using these theories, one can view a whole system as well as its details – and know where details fit into the totality. This way, one may also consciously change perspectives between totalities and some small detail, without getting lost"

Yngström (1996, pp. 31)

Kowalski (1994) suggested that ICT security can be modelled as a hierarchy of social and technical security measures. He suggested the use of the Security By Consensus (SBC) model when attempting to model both the static and dynamic characteristics of ICT security problems. The model divides the security into social and technical categories (see figure 3-3) which are further divided into sub-classes, namely, social (Ethical-cultural, Legal-contractual, Administrative-managerial-Policy, Operational-procedural) and Technical (Mechanical-electronic and Information-Data).

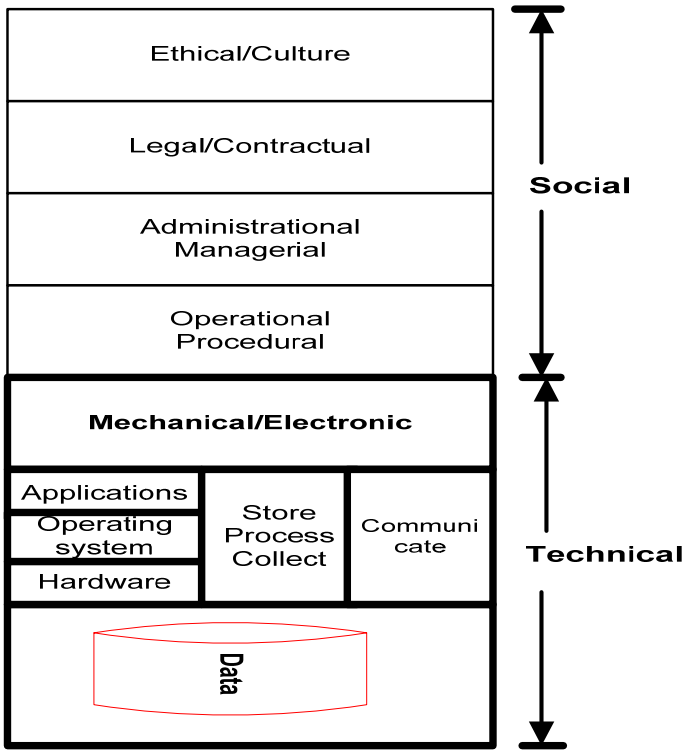


Figure 3-3: SBC Model, Source (Kowalski, 1994, pp. 19)

The two holistic models (systemic-holistic and SBC) facilitate interdisciplinary considerations when dealing with the ICT security problem.

[37] Meta: from Greek and Latin meaning between
[38] Wiener (1948) defined cybernetic as the science of control and communication in the animal and the machine. In (Schoderbek et al.; 1990, pp. 77)

To sum up the discussions in this section, one may conclude that there is a need to take a holistic approach when dealing with security problems in order to ensure that different security solutions are not applied to isolated problem areas. The scalable concept of the system theory allows the integration of the bordered parts into the whole system (Yngström, 1996; Frisinger, 2001).

3.3 Interpreting the ICT Security Management Problem

"A man's judgement cannot be better than the information on which he has based it."
(Sulzbeger, 1947)

Drucker (1993) argued that *"The diffusion of technology and the commodification of information transform the role of information into a resource equal in importance to the traditionally important resources of land, labour and capital"*

In this section we explore the ICT security management problem in a more detail. Information and communication technology (ICT) security, information technology (IT) security and information systems (IS) security are in most cases used interchangeably with information security and with computer security. Depending on where each one is used, each of these may have a different emphasis, but the common concern is the security of information in some form (electronic in these cases): hence, all are subsets of information security. On the other hand, information security covers not just information but the entire infrastructure that facilitates it uses - processes, systems, services, technology (including computers), voice and data networks.

In our work we shall adopt the *definition* presented by U.S. National Information Systems Security Glossary which defines ICT security as

Definition

> *"the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document, and counter such threats".*

Consider figure 3-4. The two systems **A** and **B** can be operated by users which may be a human or an object. Let us say the systems being operated belong to organisation Y. At one time (t=0) when both systems were new, there was no information. After time t (T=0+x) where x is time lapsed, the users of the two systems have entered (collected and processed where applicable) the valuable assets—business information (stored in the database – see the figure) of organisation Y. A database is a repository of data (can be various business records) that is used to store information of interest to the organisation in a structured format.

Definition:

> *Business Information or records refers to data and information owned by the organisation like customer records, trade secrets and strategies, policies, financial data, reports, plans, and investment portfolios.*

The information stored in the two systems is only useful if it can be communicated or exchanged and made available to users when required. The process of manipulating this information is done by means of a set of instructions (commonly known as programs or software) prepared by human beings and stored or loaded into the computer. There are two major types of these sets of instructions, namely operating systems and application systems. The former controls every task the computer carries out and manages the system's resources to optimise performance, and the latter, a program is designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of applications include word processors, databases and spreadsheets.

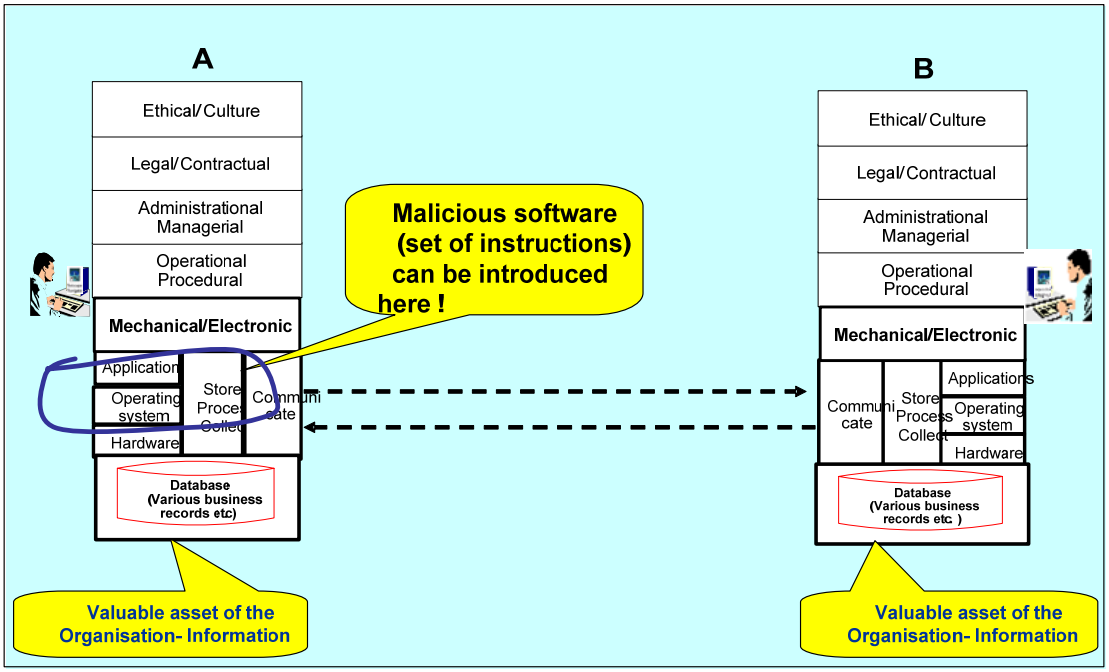


Figure 3-4: How various types of business information are being transacted

Besides the technical part, there are sets of operational procedures that guide the user on how to manipulate the process or work with the business information. Furthermore, since the two systems belong to an organisation, there will be some administrative rules on how, when and where the system operates and who operates it and for what purpose. In addition, there are legal and contractual obligations. Lastly is the issue of ethics and culture, which differs from place to place. According to (Zuccato, 2005: pp. 62) "any ethical decision is taken in a personal and social context which is the expression of a culture and of a specific social way of living". Depending on where the organisation is, this may vary.

In this scenario, the value of information, whether stored, being processed, or on transit, changes with time. Our major concern then for this business information is the availability of information or services whenever required, together with the integrity and confidentiality of the information during its lifetime. Sensitive business information should be protected from unauthorised disclosure or interception. This means that, in order to preserve the confidentiality of the business information, it should be kept secret and only be available to those who are allowed to access it.

Another important aspect is safeguarding of the accuracy and completeness of information and processing methods, because information plays a major role in the decision-making process of the organisation. If business information is not accurate or complete, it can result in poor decisions on the part of executive management. Ultimately, such decisions could lead to unwanted situations in an organisation, which could have otherwise been prevented. Ensuring the availability of information is another very important aspect to be considered, because without timely information an organisation would be incapable of continuing normal operations (Posthumus & Solms, 2004). It also means ensuring that authorised users have access to information and associated assets when required (ISO 17799). Taking the instance of availability, one of the most common ways in which the availability of information is compromised is through a denial-of-service (DoS) attack. During such an attack an information system is bombarded with a large amount of information requests, which cannot be handled by the system, and thus the system either slows down considerably or crashes, making information unavailable (Posthumus & Solms, 2004). The question here then is how one can manage the security of these organisations' information systems that handle business information, in order to minimise the possibility of systems being interrupted.

Before we start our discussion on the ICT security management approaches, a few concepts of ICT security management processes and approaches are given in the next section.

3.4 The concepts of ICT security management Processes and Approaches

As pointed out in the introduction, ICT supports the core services of an organisation and so a security management process is a fundamental requirement for any organisation whose core services depend on ICT for it to operate and survive in today's world. This process involves preservation of the confidentiality, integrity and availability of sensitive business information and is achieved by implementing a suitable set of controls which could be policies, practices, procedures, organisational structures and software functions. Security management processes have to be continuous because service requirements and security risk variables change every day. Security risk variables include threats, vulnerabilities, attack techniques, the expected frequency of attacks, organisational operations and technology. All of these variables change constantly, with the result that an organisation's management of the ICT risks requires a continuous process. Such a process ensures that the security vulnerabilities affecting an organisation's information systems are addressed in an efficient, thoughtful, timely and effective manner.

The process can start with a quick scan to determine the current state (at the time of planning) of ICT security in an organisation (Pfleeger, 2003). This is immediately followed up by a plan which covers both a description of the current situation and a plan for improvement. The plan shall then detail the risk assessments, policy development, policy implementation, administration and audit to ensure the compliance of implementation and the proposed policy (Frisinger, 2001). Figure 3-5 outlines the continuous security management process.

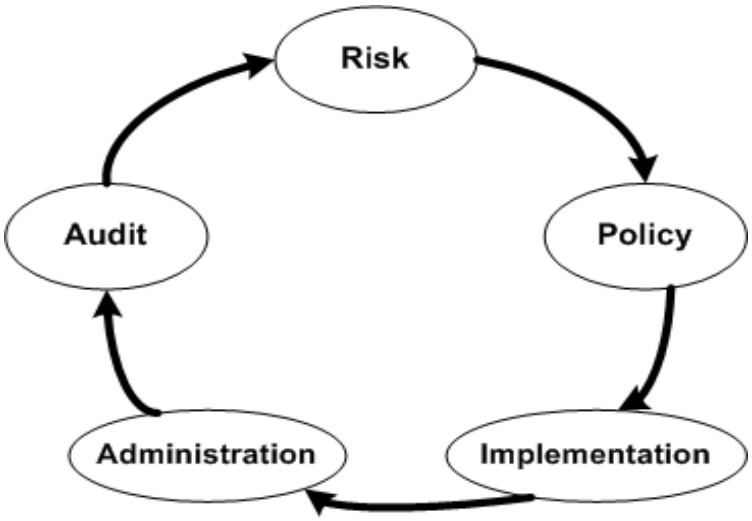


Figure 3-5: Continuous security management process (Source: Frisinger, pp. 20)

As recommended in (Frisinger, 2001; ISACA, 2005), the security management process includes the following categories:

(a) Information Security Risk Assessment and Planning: a process to identify and analyse threats, vulnerabilities, attacks, probabilities of occurrence, and possible outcomes. This process includes recommendations for improvement and provides an understanding of security requirements in the context of an organisation's current and future plans.

(b) Information Security Design and Policy: addresses security requirements by providing a plan to mitigate risks that integrates technology, policies, procedures and training. The ICT security policy provides a mechanism whereby top management can lay down a clear statement of direction and rules for the successful operation of the organisation as far as ICT security is concerned. It is important that the plan and the policy are reviewed and approved by the board of directors before implementation.

(c) Security Controls Implementation: When the design and policy have been approved, implementation follows. At this stage, the following activities take place: the selection of security products and services; acquisition and operation of technology; the specific assignment of duties and responsibilities to managers and staff; the deployment of risk-appropriate controls; assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfil their duties; ensuring that staff understand the proposed ICT security policy and its implications.

(d) Administration and Monitoring: continually administer and monitor perimeter security defences against threats. This process involves continuously gathering and analysing information regarding new threats and vulnerabilities, actual attacks on the organisation or others combined with the effectiveness of the existing security controls. Caelli pointed out that security breaches can better be managed based on three business principles which are: individual accountability, separation of duties and auditing (Caelli et al., 1991). These could facilitate in finding out what has happened and who was at fault.

(e) Audit: Finally, **audit** and **evaluate** the effectiveness of the implemented security policy and countermeasures. This information is used to update the risk

assessment, strategy, and controls. Auditing, evaluating and updating the plans and policies through risk assessment again make the process continuous instead of a one-time event.

The problem of this process though is the lack of awareness sub-process. Along with this process is the question of ICT security awareness, training and education. Human resources are the weakest link in any security chain even with the best security infrastructure in the world (Bishop, 2003). All efforts can turn out to be useless by simple social engineering, which is a result of not ensuring that staff are aware of the risks and familiar with sensible and simple security practice. Table 3-1 which indicates the reasons why ICT abuse is possible shows clearly that the problem is with people. Caelli et al. (1991) argue that information systems are vulnerable to attack by those who are in a position to abuse the responsibilities entrusted to them.

Table 3-1: Why ICT abuse is possible

Poor supervision of staff	19%
Inadequate controls over access to info. systems	13%
Inadequate or insufficient training	13%
Few checks on data from other sources	11%
Lack of Internet activity monitoring	11%
Virus detection & prevention software not installed	9%
Inadequate firewall	8%
Transactions not traceable to individuals	7%
Poor password control	6%
Lack of clarity over security responsibilities	5%

Source: (UK Audit Commission, 2001)

Similar reasons apply to the studied environment. What is the use of having an expensive firewall, intrusion detection, anti-virus etc., if someone can get what he or she wants from the target organisation through employees, as a result of, for example, poor supervision of staff or insufficient awareness and training? Giving attention to raising awareness and training ICT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure ICT resources, is therefore not optional for successful management of ICT security (Bishop,2003; Hash & Wilson, 2003; Frisinger, 2001).

The economics approach to information security

"The cost of implementing security measures must be weighed against the value of information being protected and the price of having a security incident caused by non-implementation of security measures"

(Pipkin, 2000) in (Tsiakis, 2005)

Ensuring that technology investment protects the right things is a key factor in getting value from the security (Purser, 2004; Anderson, 2001). If protection is not done properly, the organisation can face three types of economic impact as a result of a breach of security as shown in Table 3-2.

Table 3-2: Types of economic impact

	Economic impact on organisation	Consequences of impact
1	**Immediate economic impact**	• The cost of repairing or replacing systems • The disruption of organisation's services, causing un-availability or delays in service transactions
2.	**Short-term economic impact**	• The loss of contractual relationships or existing customers because of the inability to deliver services and a negative impact on the reputation of the organisation
3.	**Long-term economic impact**	• Erosion of stakeholders' confidence • Reduced goodwill

Source: (Tsiakis, 2005, pp 106)

For non-commercial organisations what is becoming crucial in addition to the list in the table is the social impact that the customer will face where the immediate impact could be the cost of an alternative solution that the customer will have to look for. For example, the adverse effects of privacy loss are borne more by those whose privacy is breached (the customer!). In economics, this is known as an externality, an effect of an organisational decision that does not affect the organisation (Schneier, 2004).

The risk-based approach to information security

Some literature has looked at the ICT security management problem as part of risk management (Blakley et al., 2001; Hamilton (1985) in (Yngström, 1996); Hill (2005). We shall in this section revisit some of their concepts.

Blakley et al. (2001) see information security as information risk management. Blakley argues that any compromise of a valuable information asset will cause dollar (shilling) losses to the information's owner; the loss could be either direct (through reduction in the value of the information asset itself) or indirect (through service interruption, damage to the reputation of the information's owner, legal liability, etc.). There is therefore a need to quantify the information security risk and the effectiveness of information security risk control measures.

In simple terms risk is a potential loss given as

Risk = Prob x Loss

Where *Prob* is the probability of a negative outcome and *Loss* is the loss through a negative outcome.

A simple and common measure for the cost of risk is Annual Loss Expectation (ALE). ALE is the expected cumulative cost of risk over a period of one year. ALE can be expressed as

ALE = *(impact of event) x (frequency of occurrence)* Source (Tsiakis, 2005)

Hamilton (1985) in (Yngström, 1996) described the concept of risks using a risk-management circle as shown in figure 3-6. He classified the risks as liability claims, environmental injury, personal injury, property damage, criminal activities and consequential losses. Hamilton further suggested that the risk manager be coordinator of all the activities shown at the centre of the figure.

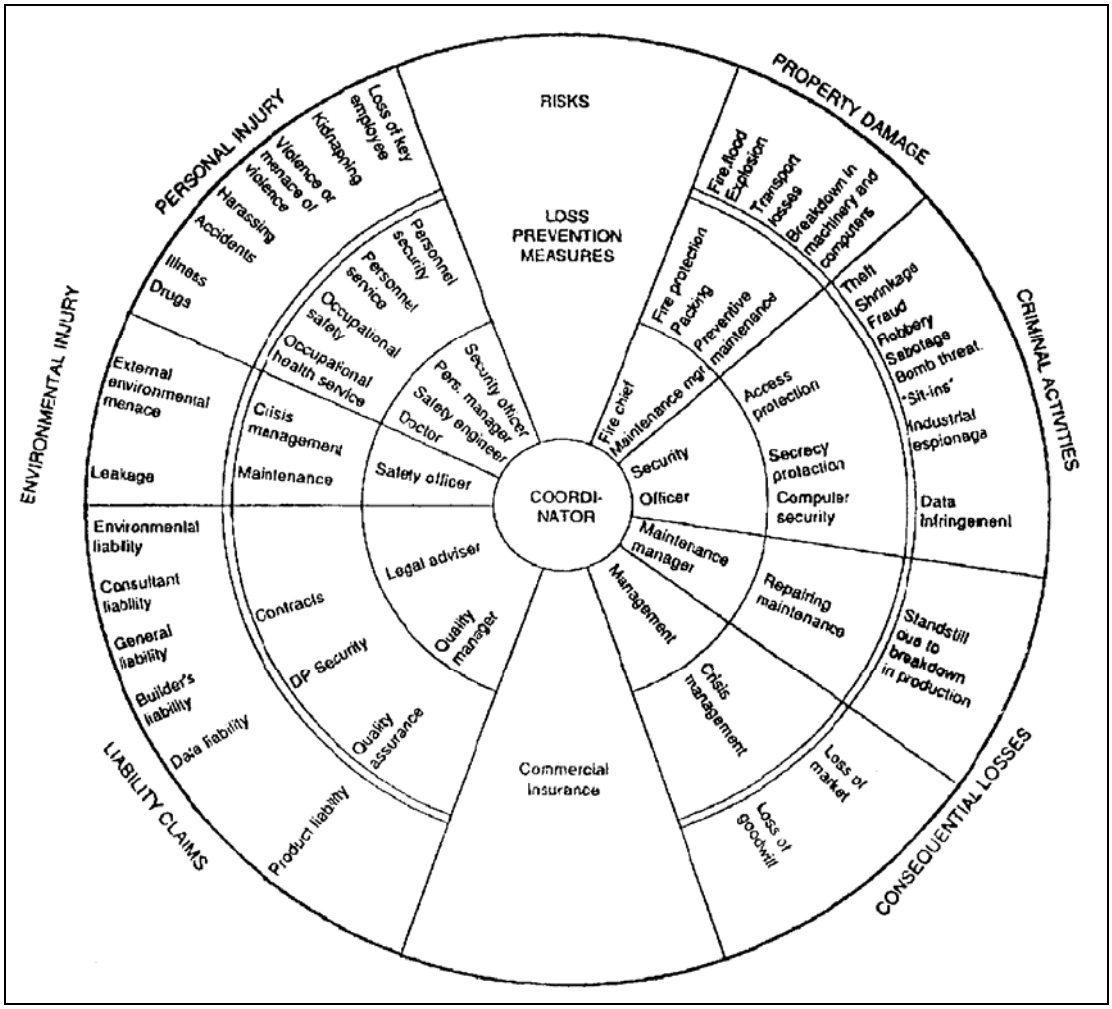


Figure 3-6: The Risk Management Circle (Hamilton (1985) in (Yngström, 1996, pp. 33)

Hill (2005) defined risk as the probability that a given threat will actually exploit a given vulnerability and cause harm as depicted in figure 3-7. Hill (2005) suggests the following terminologies for a better understanding of the nature of risk and how one could respond to it.

Some Definitions

(a) ICT Asset: *Anything of value—what we want to protect. The ICT asset in our work comprises the following:*

(i) Business Information— Data and information owned by the organisation like customer records, trade secrets and strategies, policies, financial data, reports, plans, and investment portfolios.

(ii) Systems— Information systems that process, transmit and store information. Thus software, hardware, personnel, and management together form the system.

(iii) Software— Applications and services like operating systems, databases, networking software, and other application software used by the organisation for processing or transmission of information.

(iv) *Hardware—Physical assets like personal computers, servers, CDs, hard disks, routers, and switches which are used by the organisation for the transmission, storage or processing of data or information.*

(v) *People— Expertise in the organisation, knowledge and experience which can be hard to replace.*

(Albert & Dorofee, 2003)

(b) Threat: *Anything that could harm an ICT asset*

(c) Threat agent: *Any person or thing that can do harm*

(d) Vulnerability: *A deficiency that leaves an asset exposed to harm. Vulnerability is the place where it is possible to introduce a fault. Vulnerability can be located in, e.g., the code, the configuration, or the design of the system. The presence of a vulnerability means that the system is in a vulnerable state. The critical points in a system are the places where faults are introduced, which for external faults are at the boundary between the environment and the system. All systems are vulnerable to some extent and they can experience vulnerability any time during their lifetime* (Lindskog, 2000: pp 33-34).

(e) Exposure: *Harm caused when a threat becomes real*

(f) Countermeasure: *Any protective measure taken to safeguard an asset*

(g) Attack: *An attack is an intentional activity conducted or initiated by a human and therefore is considered as an environmental influence. If the system is in a vulnerable state an attack may be successful and cause the type of fault called security breaches. A breach results in an error or a vulnerable state in which the system's security policy is violated.*

(Lindskog, 2000; Hill, 2005)

In Figure 3-7, the threat agents, threats, vulnerabilities, assets, exposure, and countermeasures are caught up in a relationship cycle.

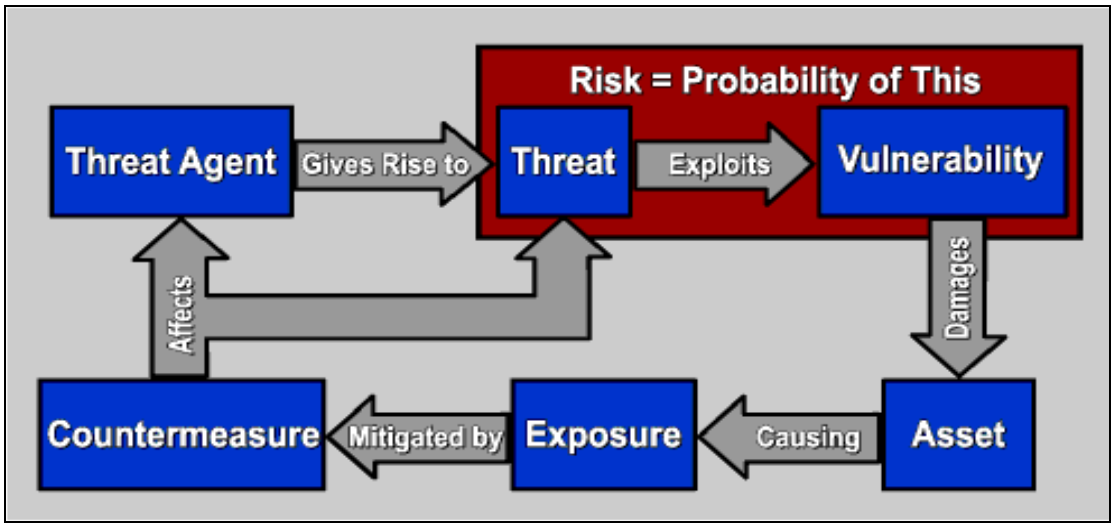


Figure 3-7 : The Cycle of Risk and its definition (Source: Hill, 2005, pp. 3)

Risks arise because an attack could exploit some vulnerability in the system which reflects a potential threat. Countermeasures can limit either a threat agent or a threat.

Depending on the ICT security management approach, the ICT security management processes differ from one approach to another. In the next section we explore a few examples of the existing ICT security management approaches and their applications.

3.5 Examples of ICT Security Management Approaches

Baskerville (1988) proposed four generations of security management approaches, namely checklist methods, systems engineering, systems modelling and social-technical approaches. Zuccato (2005) extended this list to fifth and sixth approaches namely business-technical approaches and holistic approaches respectively. He further proposed that the security management approaches be divided into those ones that can be categorised as scientific approaches (models and frameworks) and those ones that can be categorised as standard and best practices. It is not our intention to cover all the approaches proposed under each generation, but we shall discuss few of them, in particular those which are in the sixth generation and the ones that we have used in our various studies.

3.5.1 Models & Frameworks

3.5.1.1 BRITS

Business Requirements on Information Technology Security (BRITS) framework attempts to bridge the gap between top management and IT personnel. It translates the financial language to the IT and IT security languages, and vice versa. In the BRITS framework, the need for financial hedging such as insurance and technical countermeasures against ICT risks depends entirely on the effect these risks may have on the value of the organisation. The idea behind BRITS is that if an organisation greatly depends on ICT then the insurance structure is used to hedge it against the ICT risks, thereby securing shareholders' value. The insurance structure (captive structure) is used to provide the organisation's services with hedge policies (insurance) against the financial consequences of ICT risks. Thereafter, depending on the cover required, a security policy is produced for the ICT platforms that are responsible for an organisation's services. The BRITS framework uses the database called "Estimated Maximum information technology Loss" (EMitL) to suggest security policies based on the identified risks. This database makes it possible to estimate the costs of the exposure to loss inherent in an organisation's services, thereby incorporating it in the service price (Magnusson, 1999). The detailed study on how we utilised BRITS in study 2 in the five organisations is presented in Appendix G and the results of the study are presented in PAPER II.

3.5.1.2 Security By Consensus (SBC) Model

The idea behind SBC[39] is a common understanding between different stakeholders in the organisation, particularly when dealing with the security problem.

[39] See details in section 3.2

3.5.1.3 HSMF

Holistic Security Management Framework (HSMF) was developed by taking into consideration business, technique and sociology, with main focus on electronic commerce. The framework is based on a systemic-holistic approach of information security as proposed by Yngström (1996) and therefore is based on the concepts enforced by General System Theory. The idea behind HSMF is that security should be included in the business model (Zuccato, 2005).

3.5.2 Standards and Best Practices

There are already many established codes-of-practice that are essential to the process of managing information security in an organisation. Studying these multiple sets of practices and guidelines is of importance for determining and understanding the features being recommended to organisations which must be considered when managing information security. Indeed, some of these do address IT services and operational management, ICT security being part of it. We shall look through some of these practices and particularly those which are related to our work such as COBIT, OCTAVE, ISO17799 and ITIL.

3.5.2.1 COBIT

Control Objectives for Information and related Technology (COBIT) is another approach which has been developed by the IT Governance Institute of Information Systems Audit and Control Association (ISACA). COBIT is a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IT audit, control and security practitioners (ISACA, 2005). COBIT defines control as “the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected” (ISACA, 2005). COBIT positions itself as the tool for information technology management and refers, amongst many issues, to information security.

COBIT sets out 34 high-level control objectives for information and the technology that supports it. The controls are divided into four domains:

(i) ***Plan and organise:*** *This domain covers strategy and tactics, and concerns the identification of the way ICT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. This includes proper organisation as well as the technological infrastructure that must be in place.*

(ii) ***Acquire and Implement:*** *To realise the ICT strategy. ICT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.*

(iii) ***Deliver and Support:*** *This domain is concerned with the actual delivery of required services, which ranges from traditional operations over security and continuity aspects to training. To deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.*

(iv) ***Monitor and Evaluate:*** *All ICT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organisation's control process and independent assurance provided by internal and external audit or obtained from an alternative source.*

(ISACA, 2005)

The latest version[40] of COBIT focuses on regulatory compliance. It helps organisations to increase the value attained from IT. COBIT 4.0 provides guidelines for streamlined and practical activities, and enables them to achieve continuous improvement in IT governance.

3.5.2.2 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method was developed by the Carnegie Mellon Software Engineering Institute (SEI) at the CERT Coordination Centre (CERT/CC). OCTAVE is a risk-based strategic assessment and planning technique for ICT security (Alberts & Dorofee, 2003). OCTAVE is organised in three phases as follows and as summarised in figure 3-8:

(a) **Phase 1:** *Build Asset-Based Threat Profiles* – This is an organisational evaluation. The analysis team determines what is important to the organisation's information-related assets and what is currently being done to protect those assets. The team then selects those assets that are the most important to the organisation and describes the security requirements for each critical asset. Finally, it identifies threats to each critical asset, creating a threat profile for that asset.

(b) **Phase 2:** *Identify Infrastructure Vulnerabilities* – This is an evaluation of the information infrastructure. The analysis team examines network access paths, identifying classes of information technology components related to each critical asset. The team then determines the extent to which each class of component is resistant to network attacks.

(c) **Phase 3:** *Develop Security Strategy and Plans* – At this stage, the analysis team identifies risks to the organisation's critical assets and decides what to do about them. The team creates a protection strategy for the organisation and mitigation plans to address the risks to the critical assets, based upon an analysis of the information gathered.

[40] At the time of this writing

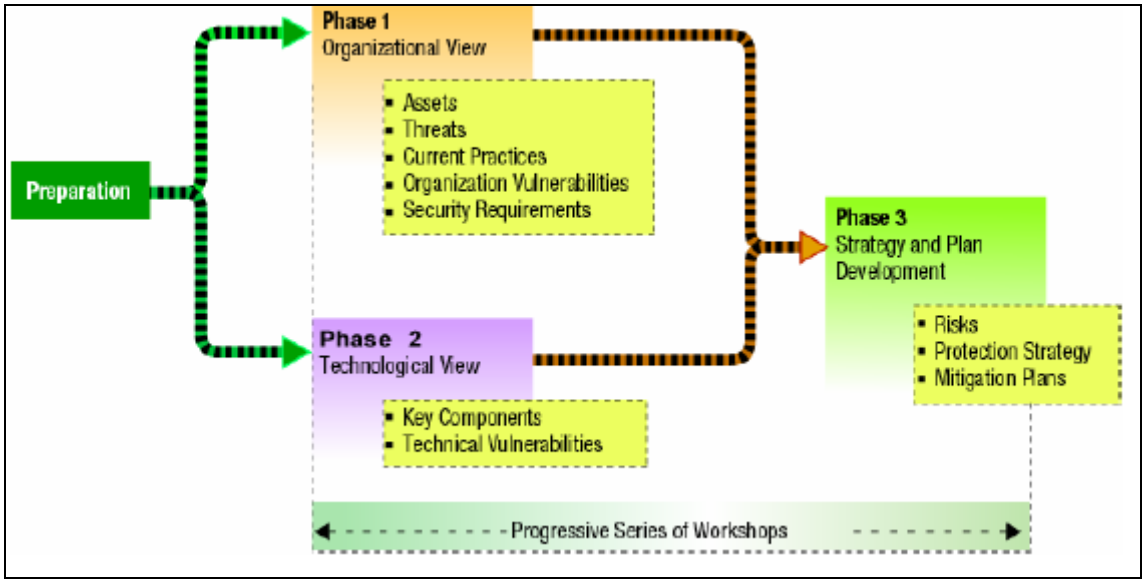


Figure 3-8: OCTAVE Phases (Source: Alberts & Dorofee, 2003, pp 44)

Although the OCTAVE method was developed for large organisations, a method known as OCTAVE-S has recently been developed for smaller organisations. The basic premise of OCTAVE is structured interviews at various levels within the organisation to identify critical assets and then determine the risks to those assets, and hence develop protection strategies and mitigation plans (Alberts & Dorofee, 2003).

3.5.2.3 ISO/IEC 27001:2005 Standard

We also have in place an internationally recognised generic information security standard, comprised of a code-of-practice and a specification for an information security management system (ISO/IEC 27001:2005). The standard sets out the requirements for an information security management system or process. It is intended to be used by organisations for identification and management of the range of threats to which information is routinely subjected.

The standard was first published as (Department of Trade Industry) DTI code-of-practice incorporating best practice based on the commonly used baseline controls in the UK. This code–of-practice was then improved to become the standard programme of the British Standards Institute (BSI) and in 1995 became BS 7799 ‘Code–of-practice for information security management’. The spread and use of BS 7799 across different sectors in and outside the UK brought feedback which resulted in the publication of a standard for specification of requirements for information security management systems named BS 7799 Part 2, in 1998. It was during that time that the original code-of-practice was renamed Part 1. Later the two parts, 1 and 2, following various discussions in the industry, were revised and published in 1999 (ISMS, 2004).

In 2000, BSI submitted BS 7799 to ISO for a fast-track vote of approval to become an international standard. During an ISO/IEC JTC 1/SC27 resolution meeting in October 2000, national body comments on this fast track were considered and BS 7799 was published as ISO/IEC 17799 in December 2000. The revision of the standard started in 2001 and the new edition was expected to be published in mid-2005. Figure 3-9 below shows the different development stages of the ISO/IEC 17799 (ISMS, 2004).

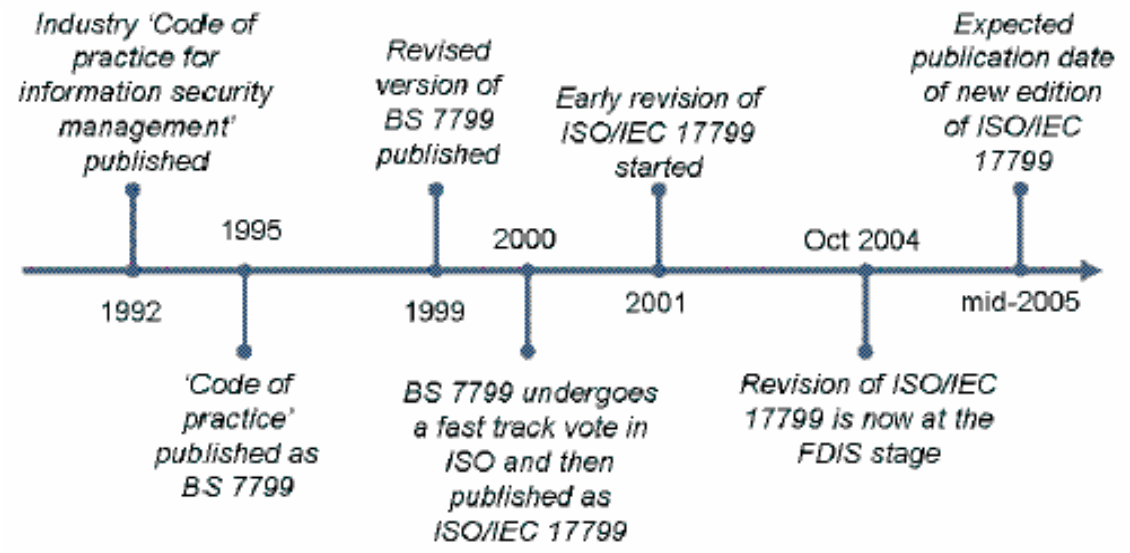


Figure 3-9: ISO/IEC 17799 (27001:2005) Development Stages: (Source: ISMS, 2004, pp. 5)

It is also important to note that ISO/IEC 17799:2000 (Part 1) is the standard code-of-practice and can be regarded as a comprehensive catalogue of good security practices. BS 7799-2 (Part 2) is a standard specification for an Information Security Management Systems (ISMS). BS 7799 Part 2 was published on 5th September, 2002. The new edition of BS 7799 Part 2 has been produced as a complement to other management system standards, such as ISO 9001:2000 and ISO 14001:1996 to provide consistent and integrated implementation and operation of management systems. The new edition standard also introduces a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing, and improving the effectiveness of an organisation's information security management system. This means how to apply ISO/IEC 17799 (ISMS, 2004).

Inside the Standard

Since we have been talking about many versions, we shall focus our observations on version ISO/IEC 17799:2000. This standard provides recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation. The standard is divided into 10 sections, with 36 objectives. Each objective is again divided into sub-objectives. The 10 sections can be summarised as follows:

(i) **Security policy:** Aimed at providing management with the direction and support for information security

(ii) **Organisational Security:** Consists of three sections. First is the information security infrastructure which aims at managing information security within the organisation. Secondly, security of third-party access, with the aim of maintaining the security of organisational information processing facilities and information assets accessed by third parties. Thirdly, outsourcing, aimed at maintaining the security of information when the responsibility for information processing has been outsourced to another organisation.

(iii) **Asset classification and control:** Consisting of two sections. First, accountability of assets with the objective of maintaining appropriate protection of organisational assets. Secondly, information classification with the goal of ensuring that information assets receive an appropriate level of protection.

(iv) **Personnel security:** Aimed at reducing the risks of human error, theft, fraud or misuse of facilities. Secondly, to ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work. Finally, to minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

(v) **Physical and environmental security:** To prevent unauthorised access, damage and interference with business premises and information. In addition, to prevent loss, damage or compromise of assets and interruption to business activities.

(vi) **Communications and operations management:** To ensure the correct and secure operation of information processing facilities, and maintain the integrity and availability of information processing and communication services.

(vii) **Access control:** To control access to information.

(viii) **System development and maintenance:** To ensure that security is built into information systems.

(ix) **Business continuity management:** Aimed at offsetting interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

(x) **Compliance:** To avoid breaches of any criminal and civil law, whether statutory, regulatory or contractual. Secondly, to ensure compliance of systems with organisational security policies and standards, taking system audits into consideration.

The purpose of ISO/IEC 17799 is to assure the confidentiality, integrity and availability of information assets of the organisation by using a set of controls, which could be good practice, policies, organisational structures, software functions or procedures. It is intended to provide a common basis for developing organisational security standards and effective security management practices that provide confidence in inter-organisational dealings (ISO 17799).

3.5.2.4 ITIL

ITIL (IT Infrastructure Library) is another widely accepted approach to IT Service Management in the world. The best practice processes promoted in ITIL are supported by the British Standards Institute's Standard for IT Service Management (BS15000). ITIL addresses IT services and operational management practices that contribute to security. It ensures that among other things effective information security measures are taken at strategic, tactical, and operational levels (ITIL, 2005).

3.5.2.5 Outsourcing ICT Security Services (MSS)

One of the possible alternatives an organisation can use to successfully manage its information and communication technology (ICT) security is to outsource its security services. This means transferring part or all of the risks management process to another organisation called a Managed Security Service Provider (MSSP). This is the same as managing ICT-related risks by transferring them to another organisation—the MSSP. Managed security services (MSS) is a service used to identify and handle organisations' real-time ICT security risks by using a proven continuous management process (IBM, 2004). Services offered by MSSPs may include: assessment of vulnerabilities; detection of attacks; protection of the ICT infrastructure and reporting suspicious activities and events; incident management, including emergency response and forensic analysis; penetration testing, anti-virus and content filtering; information risk assessments, data archiving and restoration; and on-site consulting services. An example of such services is network boundary protection which includes managed services for firewalls, intrusion detection systems (IDSs), and virtual private networks (Allen et al., 2003; Sadowsky et al., 2003). In practice, the service/s offered will depend on what was requested and bargained for in the contract, as not all these services are necessarily included.

Such services, whether outsourced or provided in-house, are critical for the reliable state of security of an organisation whose core services are directly linked to the state of its information systems. However, while outsourcing is one of the solutions that are recently emerging, a careful analysis of its advantages and disadvantages should be considered before attempting to make any decisions. It is true that, given the nature of the ICT security problem (multi-dimensional one), organisations need to have in place the right technology, experienced people, continuous monitoring, and continuous threat intelligence, in order to implement and maintain sufficient security in an organisation. Depending on the size of the organisation and its dependency on ICT, it may be difficult to cope with the huge quantity of information about security threats, which includes among other things monitoring thousands of logs from a number of devices, and responding quickly to security events. That is a challenge, particularly for organisations whose core service is not ICT or security itself, and this is where the idea of outsourcing is coming from (Magnusson, 1999; Allen et al., 2003). There is therefore, a need to clearly explore the benefits and consequences of outsourcing, before one makes a decision on whether or not to outsource ICT security services.

3.5.2.6 The balanced scorecard (BSC)

> *"…financial measures tell the story of past events, an adequate story for* ***industrial age*** *companies for which investments in long-term capabilities and customer relationships were not critical for success. These financial measures are inadequate, however, for guiding and evaluating the journey that* ***information age*** *companies must make to create future value through investment in customers, suppliers, employees, processes, technology, and innovation…"*
>
> (Kaplan & Norton, 1990)

The balanced scorecard is another management system methodology which, although not confined to ICT security, enables organisations to clarify their vision and strategy and translate them into action. This approach to strategic management was developed in the early 1990's by Drs. Robert Kaplan (Harvard Business School) and David Norton. The balanced scorecard suggests that we view the organisation from four perspectives as summarised in figure 3-10.

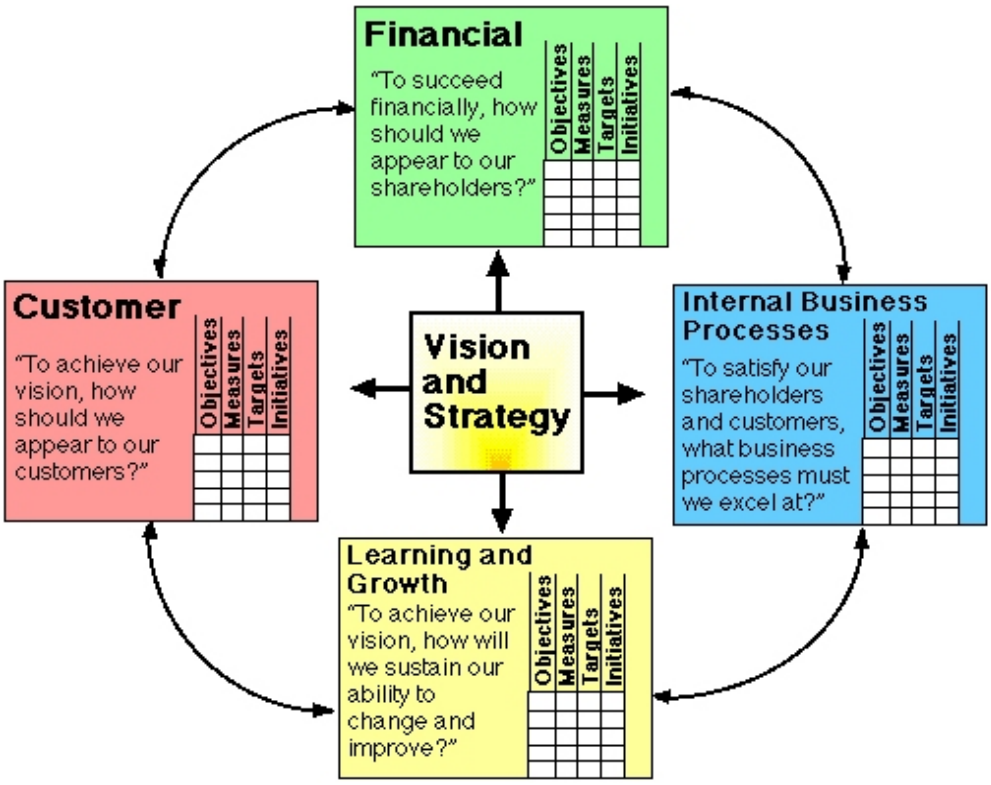


Figure 3-10: Balanced scorecard (Source: Kaplan & Norton, 1990)

(i) **Learning and Growth:** This perspective includes employee training and corporate cultural attitudes related to both individual and corporate self-improvement. In the information age, it is becoming necessary for employees to be in a continuous learning mode.

(ii) **Business Process:** This perspective refers to internal business processes which include mission-oriented processes and support processes.

(iii) **Customer:** Customer *focus* and *satisfaction* are now very important factors in any business. If customers are not satisfied, they will eventually find other suppliers that will meet their needs. Poor performance from this perspective is thus a leading indicator of future decline, even though the current financial picture may look good.

(iv) **Financial:** There is always a need for timely and accurate funding data. With the implementation of a corporate database, it is expected that more of the processing will be centralised and automated. According to Kaplan & Norton

> (1990), the current emphasis on financials leads to the "unbalanced" situation with regard to other perspectives. There is therefore a need to include additional financial-related data, such as risk assessment and cost-benefit data, in this category. **Kaplan & Norton (1990)**

The balanced scorecard provides feedback about both the internal business processes and external outcomes in order to continuously improve strategic performance and results in the organisation. We found the four perspectives very useful concepts when building an ICT security programme in the organisation.

3.5.3 Summary of the section

Certainly, this is not an exhaustive list of the existing ICT security management approaches, but they are currently among the widely accepted approaches for managing ICT in general and ICT security in particular. There are many more existing approaches such as those suggested by the American National Institute of Standards and Technology (NIST) and various national (in different countries) standard and directives for managing ICT security. There are also other methods like the Common Criteria (CC[41]), which combines the best aspects of existing criteria for the security evaluation of information technology systems and products. The idea behind CC is that confidence in ICT security can be gained through actions that may be taken during the process of *development, evaluation* and *operation* (CC, 2006).

Going through these approaches one of the observations is that they have different orientations, which sometimes depend on where they originated and where they were first applied. Table 3-3 summarises the different orientations for each approach.

Table 3-3: Orientation of different Approaches

	Approach	Comments on the Orientation of the approach
1	BRITS	Risk management oriented – Insuring ICT risks
2	SBC	Social-Technical process
3	HSMF	Holistic Security Management – for electronic commerce
4	COBIT	IT governance process
5	OCTAVE	Risk evaluation
6	ISO 27001	Process (Information security) oriented
7	ITIL	Process (IT management) oriented
8	MSS	Risk Management by transferring to the third party
9	BSC	Management Process (business-driven) oriented

All these approaches or orientations contribute to the management of the ICT security problem, which indicates that there is a synergy in combining more than one approach that is they can complement each other. For instance, the BRITS framework was very useful here for interpreting financial terminologies (financial risk exposure) to corresponding ICT security terminologies (countermeasures). Likewise by making use of the SBC model, it was easy to see different parts (holistic view) of the problem and hence we used it in different studies as a basis for interpreting the problem in the process of addressing the perception problem. More examples of the benefits of

[41] The Common Criteria work is an international initiative by the following organisations: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA).

combining more than one approach are shown in our study 5 (PAPER VI) and also by Solms (2005) and (itSMF, 2006).

3.6 Discussion and Conclusion

In this chapter, we have gone through the General Systems Theory and the concept of holism. We have also investigated the ICT security management problem in a more detailed way and revisited some of the existing ICT security management approaches. We found that the approaches can be categorised into two major groups, those which are models or frameworks which, according to Zuccato (2005), can further be grouped into six generations, and those which can be categorised as best practices or standards. The latter approaches are derived from the first group (models and frameworks) and experience gained in practice over time. The main difference between the two groups is that the first one is at a high level—more abstract, and the second is less abstract and can more or less be applied directly to the problem with minimum customisation. Further analysis showed that these approaches have some kind of different orientations as summarised in table 3-3.

The first observation we can draw from the discussions in the chapter is that the theoretically holistic approach referred to as sixth generation has generally been recommended for the management of ICT security problems (Kowalski, 1994; Yngström, 1996; Magnusson, 1999; Frisinger, 2001; Eloff et al., 2003; Zuccato, 2005). We however learnt from study 2 that some prerequisites are required before using these approaches. One has to customise the existing approach or use more than one approach to address the observed ICT security management problem. Our experience during the studies indicated that, the customisation process and use of different approaches without some sort of a guideline may complicate the problem even further. For example, we have seen in study 1-Paper I and study 2-Paper II, III, appendix G and H that the use of the existing approaches such as BRITS, best practise such OCTAVE and Outsourcing depended very much on the customisation of the approaches. This customisation process and use of different approaches required high expertise, which is also a problem in the studied environment. Moreover, the environment in which the studied organisations are located, public infrastructure such as education institutions lacked courses on ICT security and hence there is a low level of awareness of the ICT security problem. This is a situation which calls for an approach where awareness and consequently the perception problem as detailed in Paper I, are addressed.

The second observation is the gap between the focus of the investigated approaches discussed above and observed situation-specific problems in the studied environment. For example, we found in the first study that the ICT in the studied environment is at the take-off stage and that none of the organisations were previously in the habit of actively incorporating ICT security into their strategic plans. At the operational level the study indicated that the complex problem of ICT security has been relegated to the IT department or ICT vendor or supplier. In other words it was treated rather as a technical problem, with no relevant organisation-wide ICT security policy. Referring to systems theory, this is partly a problem of the studied environment as detailed in Paper I and Paper V. In the third and fourth studies which were focused on the challenges when addressing such a problem, it showed that we cannot just address the

problem internally without taking into consideration the environmental factors which may also affect the ICT security management approach processes.

Based on theoretical and practical observations, we have investigated ICT security management problems and the relevant approaches available to solve them. We can summarise the discussed approaches in this way: - Both BRITS and HSMF are holistic approaches with the former mainly focusing on the insuring ICT risks, and the latter one mainly focusing on e-commerce. SBC is a model that views ICT security problem as a social-technical one and BSC is a general system management methodology which is business-driven. On the other side COBIT, OCTAVE, ITIL and Outsourcing are among the best practices which are derived from various models and generations, with different orientations as summarised in table 3-3, while ISO 27001 is a generic information security management standard. For example OCTAVE approach is more on the risk evaluation and it ends up with security strategies and plans. It does not say how the developed strategies and plans can be operationalised. In addition, the Outsourcing as detailed in the second study (Paper III), could only address part of the problem—the technical one. There is therefore a need to have an approach that is easier for the management to understand and follow in addressing the observed ICT security problem in the studied environment.

In order to address this discrepancy, we decided in our approach to view the whole problem of ICT security management as a system. From this perspective the following features become apparent; the objective of the total system together with the performance measures, the environment, resources, components and management of the system. They will all become known and be made clear, thus also addressing problems such as the perception. Based on the General System Theory, a system should be holistic. Since our problems here are viewed as a system then we propose a holistic approach in dealing with them.

In the next chapter the proposed holistic approach for managing ICT security in non-commercial organisations is presented. The approach addresses the ICT security management problem as identified in the studied environment.

Chapter 4

4. A holistic Approach for Managing ICT Security in Non-Commercial Organisations

This chapter presents and describes the overall proposed holistic approach for managing ICT security in non-commercial organisations and the processes involved in each component or object that makes up the entire approach to perform as a whole. The proposed approach is based on the General Systems Theory, observations made in the five studies and to some extent also based on the existing approaches, in particular the BRITS framework, the SBC model and where appropriate standards and best practices to cover the missing links.

4.1 Framework for managing ICT Security in Non-Commercial Organisations

The framework can be considered as a system made up of 12 components and a defined environment. Each component is a sub-system characterised by inflow, throughflow[42] and outflow. In practice each of these components can be regarded as a guideline. The 12 components are organised into two phases namely, initialisation phase, and internalised and continuous phase. The initialisation phase is made up of four components or objects essential as a first step in the introduction of the ICT security management process in the organisation. The outputs of the first phase are input to the second phase, which once operational in the first circle, becomes an internalised and continuous process. The second phase is made up of eight components or objects as shown in figure 4-1. Each object is triggered by some kind of input from another object and after the process we have some kind of output which becomes input in the following step and sometimes also the feedback to other objects of the framework.

The proposed framework, summarised in figure 4-1, follows the systemic holistic approach's principles as suggested by Yngström, (1996: pp. 92) which includes;

- ✓ Delimiting the system of study from the environment,
- ✓ Defining the existing environment,
- ✓ Defining the inflow, throughflow, and outflow, and
- ✓ Structuring the built-in control system so that it can deal with inner and outer variety,

as shown in figure 4-1 and detailed in the following sections.

[42] Throughflow here means "process"

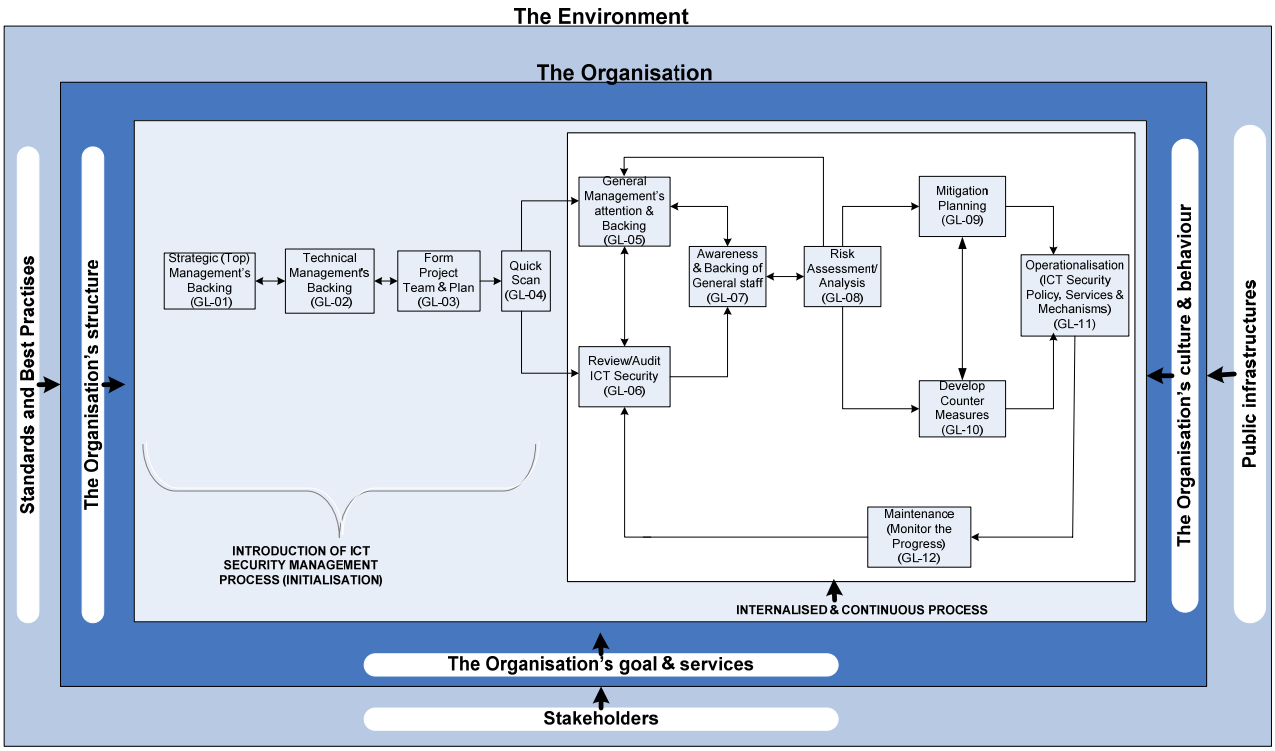


Figure 4-1: Framework for Managing ICT Security in Non-Commercial Organisation

4.2 Framework Explained

Each component's activities are executed by taking into consideration a holistic view of the ICT security problem (see figure 4-2) using the SBC model in order to have built-in security in a holistic way. In this way, the multi-dimensional nature of the ICT security problem is also incorporated.

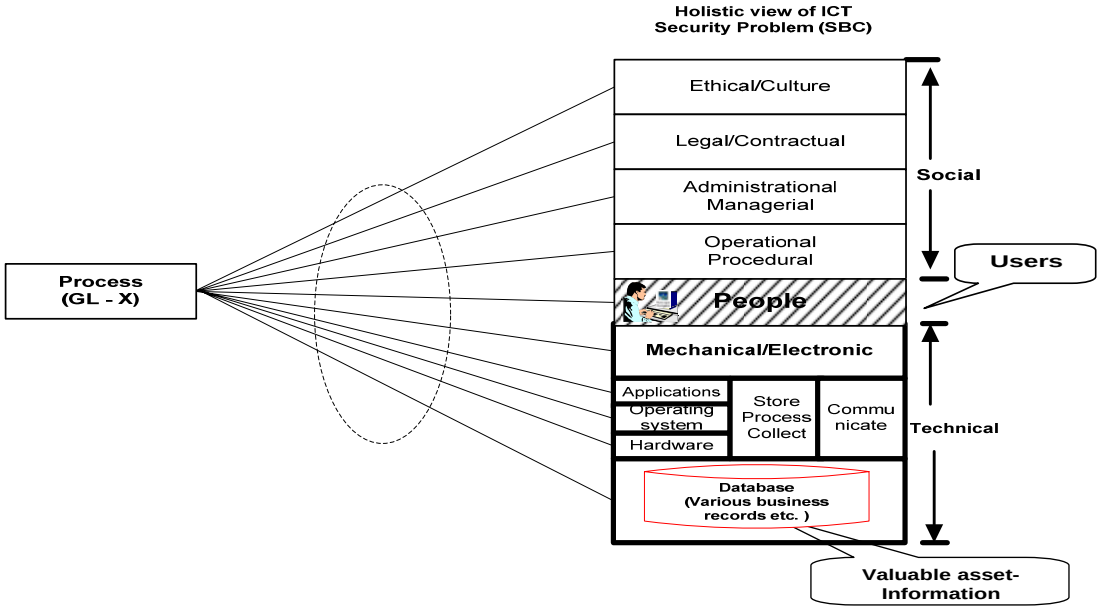


Figure 4-2: Process activities incorporating the Holistic View (SBC model) of the security Problem

4.2.1 The Environment

According to Schoderbek et al., (1985), the environment of a system includes not only that which lies outside the system's complete control but that which at the same time also determines in some way the system's performance. We shall in brief describe the components of the environment to be considered next.

Standards and Best Practices: These include standards such as ISO 27001/2 (International standard for Information Security Management), and also best practices such as COBIT, OCTAVE and ITIL.

Stakeholders: These include customers of the services provided by the organisation, employees, other organisations and the general public.

Legislation and other Public infrastructure: Public infrastructures include things such as the education system of a country, legal framework, and different physical infrastructures such as telecommunications and power. The list also includes various legislations, regulations and standards, both local and international for the organisations to conform or be compliant to. We have seen from example, the impact of the Sarbanes–Oxley Act in the US on information security for listed companies and also the government agencies (ITGI, 2006).

"Sarbanes-Oxley has forced companies to develop a continuous control-monitoring culture"

(Kumar, 2006: pp. 41)

Bodies like Tanzania Communication Regulation Authority (TCRA) and the Tanzania Bureau of Standard (TBS) are good examples of government bodies found locally in the studied environment which can put in place similar acts that would have an impact on an organisation's ICT security management process.

Organisation: This is the very environment in which the ICT security management we are referring to is going to be implemented. The structure depends on the nature of the organisation and the type of services it offers, but in principle we have departments which are further broken down into sections and sub-sections. According to Schoderbek et al (1985), these are low-level systems with respect to the organisation. We may also have various information systems within the organisation for instance a pay-roll system, a human resource information system, financial information systems, etc., which are also low-level systems with respect to the organisation or in other words they are sub-systems of the organisation. Furthermore, organisation's culture and behaviour are also very important factors to be taken into consideration when managing ICT security in an organisation. We do not address it independently in the framework, but rather it is taken care of in the processes.

In the same way that temperature, atmospheric pressure and other parameters that need to be at a certain level or adjusted to a particular level for living organisms to survive, the discussed parameters in the environment need to be available and adjusted to the required level for the proposed system to operate at optimal level.

4.2.2 Initialisation Phase

This phase consists of four components which are characterised by the backing of top management and technical management and the formation of a project team which involves senior staff from various departments. In addition, this is where the planning for the internalised and continuous process takes place.

4.2.2.1 Getting Strategic Management's Backing (GL-01)

Strategic (Top) Management's Backing (GL-01)

Top management backing is important in any effort to improve security in organisations as suggested by (Solms & Solms, 2004; Solms, 2005; Alberts & Dorofee, 2003; Caralli, 2004). It is also an important factor in corporate governance as discussed in Control Objectives for Information and Related Technologies (COBIT) by ISACA. CEOs and their equivalent in the public sector need to be educated in the consequences of not managing ICT-related risks, for stakeholder value and in their responsibility to their boards for the state of ICT security in their organisations. There is a need to show how exposure to such risks can affect the key performance indicators of the organisation and prevent it from reaching its mission and service or business objectives. In an organisation whose services depend on information systems, information security spans every division and department in that particular organisation. According to (CISM, 2006), any initiative that affects so many people and business processes cannot be successful without senior management support and commitment. Therefore, if top management do not buy into the idea, then it is most likely that the ICT security programme will fail.

4.2.2.2 Getting Technical Management's Backing (GL-02)

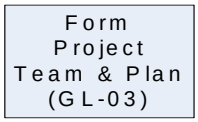
Technical Management's Backing (GL-02)

Since this complex problem of ICT security has been relegated to the IT department or rather treated as a technical problem, there is a need to get the technical management's backing. During this stage the attention has to be on getting technical management and staff to understand the non-technical components of the problem and how to communicate the problem to the management as risk exposures. They need to understand the holistic nature of the ICT security problem and why non-technical departments should be involved in the ICT security management programme.

4.2.2.3 Setting up the special ICT security project team (GL-03)

"Organisations can no longer be effective in managing security from the technical sidelines. Security lives in an organisational and operational context, and thus cannot be managed effectively as a stand-alone discipline. Because security is a business problem, the organisation must activate, coordinate, deploy, and direct many of its existing core competencies to work together to provide effective solutions."

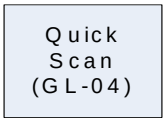
(Caralli, 2004)



The third process after succeeding in getting the backing of the top management and technical management, involves setting up a special project team and planning. The idea of setting up a project team is to be able to bring together senior staff from different discplines in order to accommodate the holistic nature of the ICT security problem, and to be able to plan and control the proposed ICT security management processes so that the system's objective can be achieved. It is proposed that the composition of the team should include senior technical staff (software, network and hardware), legal officer, internal auditor, security officer, and staff from operational departments (where core services of the organisation are processed) and, where applicable, staff from the risk management or insurance department purposely for risk management. When the team is in place, it may require a brief orientation and then the following task is to draw up a plan for the entire internalised process. In the first circle, the team may be led by an external expert who is knowledgeable about the entire process. In a way the first round can also be considered as building internal capacity.

Selection criteria: It is important to select staff who have spent a substantial amount of time in the area of consideration and who are also ICT literate, for example, a senior auditor with some general computer knowledge.

4.2.2.4 Quick scan of the ICT-related risks and their consequences for the organisation (GL-04)



There is a need to have some facts on the likely consequences of ICT-related risks for the organisation before meeting the management as a whole. This can be achieved by carrying out a quick scan of such risks with the help of the ICT security team. This exercise involves gathering information on what the organisation is doing and how its core services are linked to the use of ICT, and hence what kinds of existing risks it is exposed to and their consequences for the organisation. In order to be able to extract such information, face-to-face interviews with the CEO, chief financial officer (CFO), IT managers, system administrators and the heads of the departments involved in the provision of the core services, should be conducted. The collected information can then be used to figure out how the organisation's mission and business objectives are supported by ICT assets and in turn what are the possible risks to, and consequences for, the organisation's business objectives. We can also make use of software tools such as the EMitL tool, as suggested in the BRITS framework.

4.2.3 Internalised and Continuous Phase

Once the initialisation phase which involves component GL-01 through to GL-04 is complete, the output will be the input required to initiate the internalised and continuous phase as shown in figure 4-1.

4.2.3.1 Getting General Management's attention and backing (GL-05)

General Management's attention and backing (GL-05)

General management is used here to mean a team of senior staff who are in charge of various departments in the organisation. General management is in principle part of the decision-making system of the organisation, forming a multi-disciplinary sort of team since they come from different departments. These people need to be convinced and understand that their organisation is vulnerable to ICT-related risks. Depending on the set-up of the organisation, typically such a team may constitute the CEO, CFO, directors from various units, human resources manager, chief legal officer, chief security officer, chief internal auditor, operational manager, planning and investment manager, technical managers and other CXOs[43] and managers. They should be well informed about the magnitude of the security problem and their roles in managing the problem with respect to their positions in the organisation. Again making use of the holistic view of the ICT security problem (SBC) will help in bringing together the management team as shown in figure 4-3.

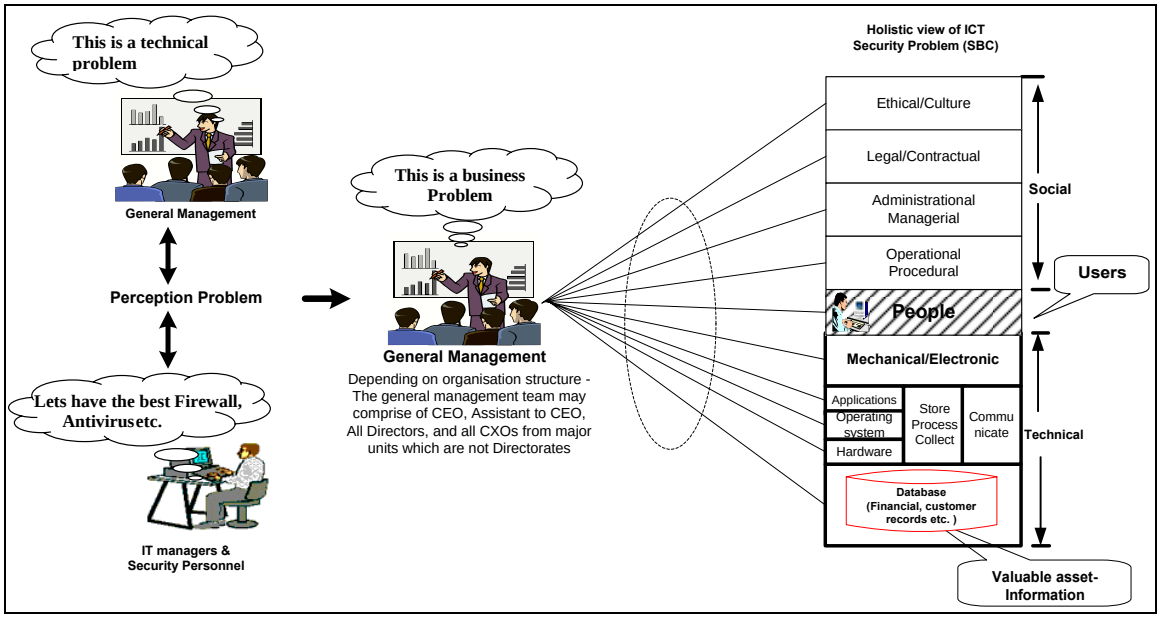


Figure 4-3: Management team discussing ICT security Problem

[43] X Refers to Officers in chief or senior positions

4.2.3.2 Audit and Review the Status of ICT security and document (GL-06)

Review/Audit ICT Security (GL-06)

Getting people to understand the status of ICT security is also a very important component in the overall management process. As shown in figure 4-1, this can be an extension of process (GL-03) or be triggered by an input from process (GL-12)—maintenance. This exercise involves taking stock of what exists in terms of: Systems (hardware, software, platforms, networks, applications, users and assets); Environment (location and services); Security (threat types, countermeasures) that are currently in place as well as potential ones; and Procedures (any policies and procedures in place). Such information helps to identify the current status of ICT assets, their location and the type of services they provide, as well as threat types for each identified asset and the security measures that are in place. Audit review takes into consideration governance controls within the ICT department, information systems security controls, ICT disaster contingency planning including the ICT elements of business continuity planning, etc. There are various ways of conducting this exercise such as OCTAVE phase 2, process 5 as detailed in (Alberts & Dorofee, 2003, pp 49). OCTAVE phase2 deals with identification of key components of an organisation's information system. This exercise also provides more knowledge of ICT assets, their link to the organisation's mission and business objectives and can help to highlight areas that need immediate attention. In addition, such information can later be used during the awareness-raising sessions (process GL-07) to help staff understand and appreciate the types of ICT security problems they have.

Maturity Models such as COBIT (CMM) can be deployed during this stage as well to control and monitor the ICT security management process. In this way management can map the organisation's ICT security status after each circle against the previous status and against best practices where necessary, which means after each feedback from (GL-12).

4.2.3.3 Conducting awareness-raising sessions (GL-07)

Awareness & Backing of General Staff (GL-07)

Most security problems are centred on people—staff (Bishop, 2003). After getting support from the management as a whole, and increasing their knowledge of ICT assets and their link to the organisation's mission and business objectives, the next stage is to conduct awareness-raising sessions for all staff. A top-down approach, starting with the senior management, line management and later general staff is recommended. Apart from the general awareness-raising session, there is also a need to have special sessions with individual departments, such as legal, accounts, internal auditing, physical security, human resources and technical, etc. Backing of general management and staff is a must and very important as an input to the next component GL-08.

4.2.3.4 Carrying out risk assessment and analysis (GL-08)

Risk Assessment/ Analysis (GL-08)

Risk assessment is another building block of ICT security management. As suggested in (Magnusson, 1999; Alberts & Dorofee, 2003), the need for countermeasures against ICT risks depends entirely on the effect these risks may have on the organisation's mission and business objectives. It is expected that after the awareness-raising sessions in the previous process, staff would have been well informed about what kinds of risk they have, their impact on the organisation and the need to have a security management programme in place. Figure 4-4 shows how the risks and their consequences for the organisation's services are derived from the organisation's objectives.

(i) Identification of Organisation's Objectives

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

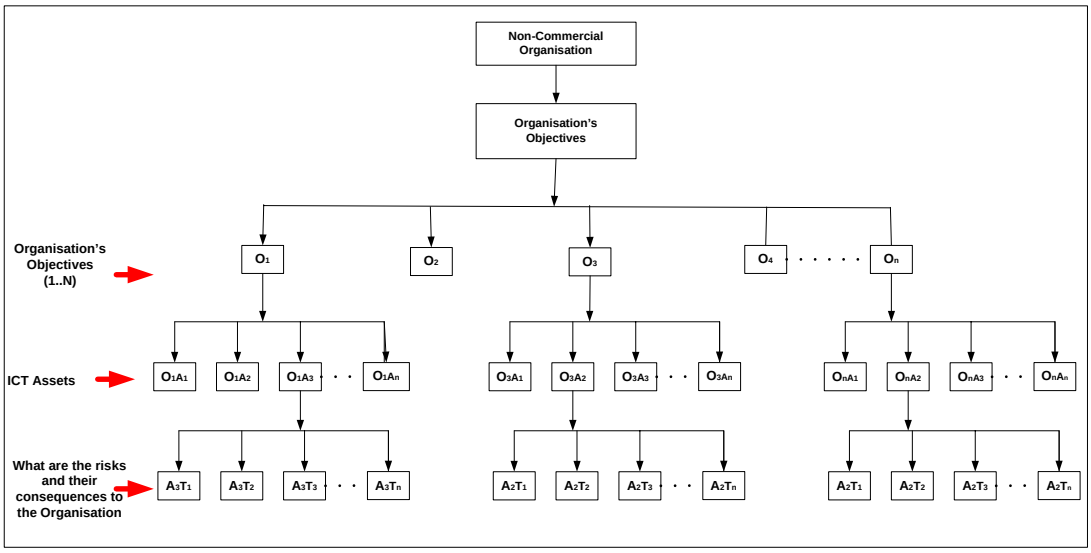


Figure 4-4: Deriving Risks to, and consequences for, the organisation's business objectives

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

The second stage involves identification of ICT assets that support the organisation's objective/s (**O_x A_x**) and the 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 ICT assets. As discussed in (Alberts & Dorofee, 2003), an 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 (**A_xT_x**) and their consequences that hinder the organisation from meeting its intended objective **O_x** (where **x** identifies the objective and likewise the corresponding threat, and can be from **1** up to **n** threats) takes 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).

4.2.3.5 Working out the Mitigation plan (GL-09)

Mitigation Planning (GL-09)

A major outcome of the ICT risk assessment and analysis becomes input to mitigation planning process. Through guideline GL-07 and GL-08, we have well informed staff, backing from the management, and the results of the risk assessment which give the status of ICT security in the organisation. After this, the development of a mitigation planning is suggested. There are two types of mitigation plan - those that address issues which will need immediate attention and those that address long-term requirements. Examples of short-term plans or things that need immediate attention can be proper patching management and complete documentation, etc. A long-term plan can include, among other things, a disaster recovery and business continuity plan, and developing countermeasures which include policies and various mechanisms and procedures for ICT security. An example of this process is OCTAVE method process 8 which involves developing a protection strategy to work out the mitigation plan.

4.2.3.6 Developing countermeasures (GL-10)

Develop Counter Measures (GL-10)

The goal here is to design and develop countermeasures tailored to the organisation that will remedy the identified vulnerabilities and deficiencies as per the plans as briefly discussed in GL-09. The use of standard and best practices such as ITIL, ISO 17799 and COBIT is very important during this stage. Figure 4-5, which is an extension of figure 4-4, shows how the countermeasures are derived from the identified risks. First the policies are developed, and then the corresponding ICT security services and finally the mechanisms required to implement the security services are proposed.

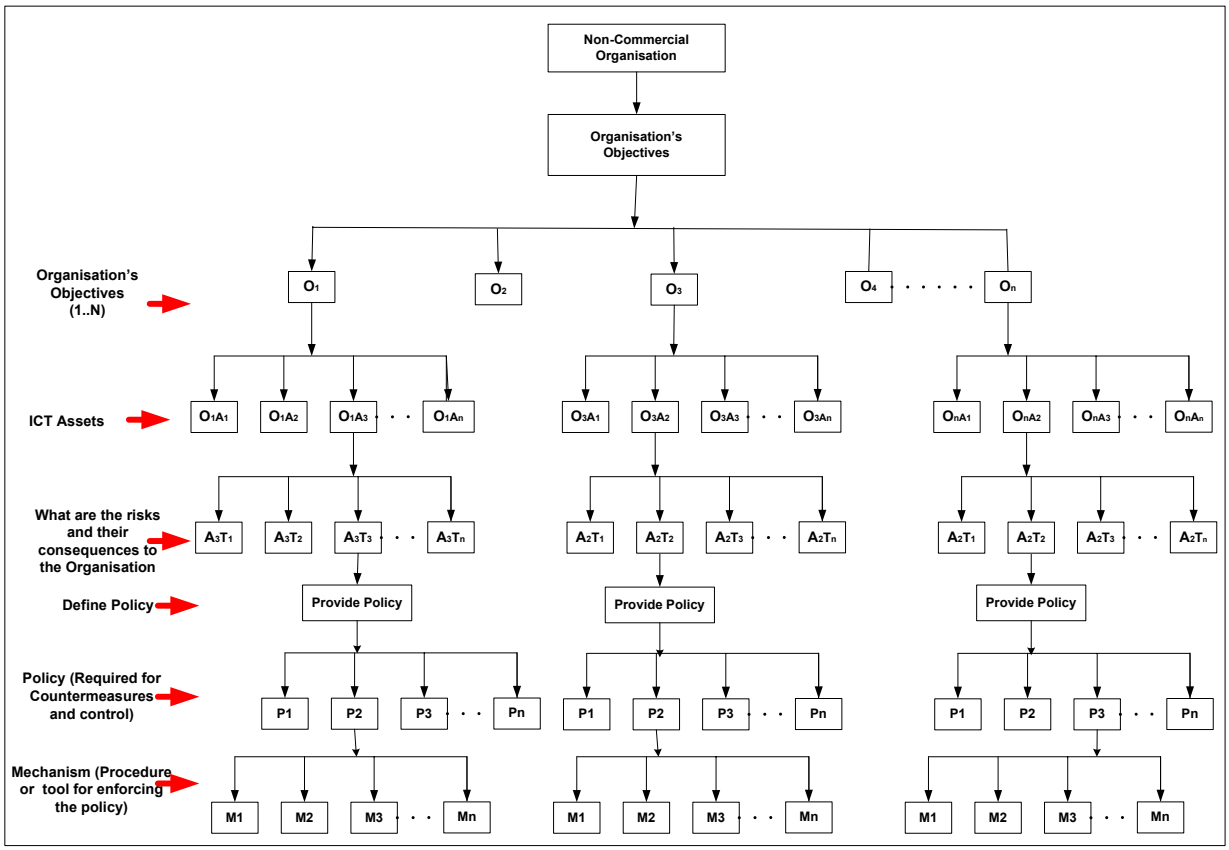


Figure 4-5: Showing how countermeasures can be derived from the identified risks

4.2.3.7 Operationalisation of ICT Security Policy, Services and Mechanisms (GL-11)

Operationalisation (ICT Security Policy, Services & Mechanisms) (GL-11)

After GL-09 and GL-10, which are mainly analytical, the solutions are still "on the drawing board", the process referred to in Information Security Management Systems (ISMS) (Bjorck, 2001). The operationalisation stage takes the conceptual levels and makes them work in the organisation. A major outcome of the ICT risk assessment and analysis is the mitigation planning which includes the countermeasures proposed for the identified problems. These are inputs into GL-11 which become the basis for the development of an ICT security policy, services and mechanisms for the organisation. In principle, for each identified problem a policy statement was proposed. For each policy statement (what), you have the objective (why), which attempts to answer the question as to why the organisation should have such a security policy statement in the policy document. The ICT security policy alone will not suffice without security services and corresponding mechanisms on how the proposed policy should be effected. ICT security policies are qualitative—statement of intent; they do not say exactly or specifically how the proposed policies should be put into practice. It is therefore important that services such as intrusion detection and mechanisms such as intrusion detection systems are more explicit and where possible explained quantitatively, so that the policy is easy to implement, enforce, measure and audit (Bishop, 2003, Peltier, 2002). In figure 4-6, we show how the policy can be mapped

to security services, mechanisms and resources. For each security service *S*, there must be at least one mechanism *M* to support it and this mechanism or set of mechanisms which may have sub-mechanisms as well must be assigned to resource *R* in a particular department. The resource can be located in a technical or non-technical department. The mechanism can be a procedure and tools (e.g. ant-virus or hardening of operating system security) to be used and the resource can be a member of staff.

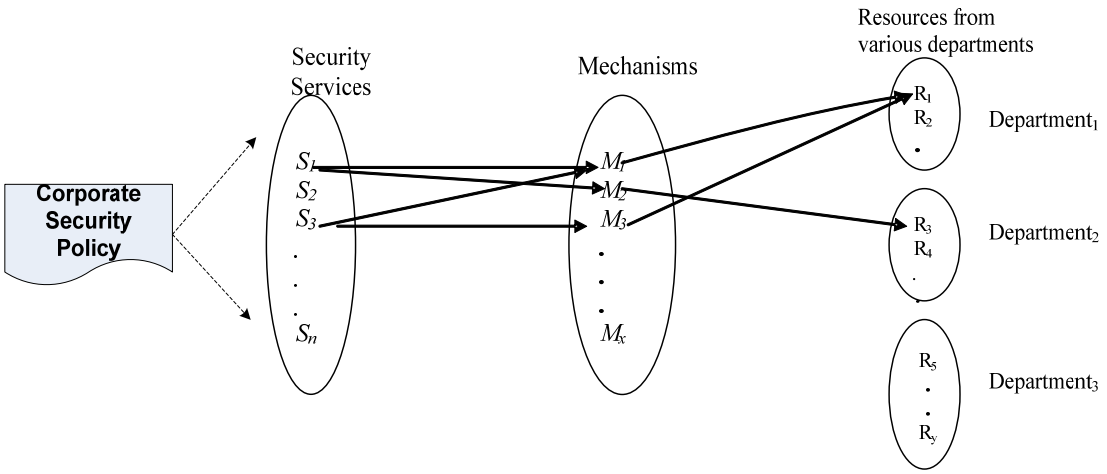


Figure 4-6: Mapping Policy, Services, Mechanisms and Resources

For example, if one proposes a policy statement which will result in a security service such as data replication and back-up, the corresponding mechanism will be the actual back-up of, for instance particular business records. This must then be followed by routine procedures which show what are the type of data or systems (whether critical or not), how frequently the back-ups should be taken and whether they are on- or off-site, and what resources are required. In turn these procedures should be reflected in the roles and responsibilities of a particular department and consequently reflected in somebody's job description. Now since we know the type, volume and sensitivity of data, we can then have a clear indication of what type of back-up facilities should be in place. In addition, one must make sure that the person responsible for this back-up process actually knows how to go about the process.

This process may call for the re-structuring of some departments, and which leads to redefining the individual job-descriptions of staff so that they can assume the new role of ICT security. This in turn calls for specialised trainings, awareness-raising and reorientation sessions and, where necessary, recruitment of new personnel. It is important that the entire process is carried out in a cost-effective way and all financial and resources implications should be reflected in the short and long-term plans of the organisation. Awareness and backing of senior management, general management and staff is very important for the success of this process. There is also a need to clarify the question concerning overall ownership of the ICT security function within the organisation so that at the end of the day we have a real owner. If placed in the right position in the organisational structure, the overall owner of the ICT security function can have the authority to oversee and control security throughout the organisation. This is very important if we are to succeed in the entire process of operationalisation

of the ICT security policy, services and mechanisms. A more detailed discussion on how these can be practically achieved is presented in PAPER VII.

4.2.3.8 Maintenance - Monitor the Progress (GL-12)

Maintenance - Monitor the Progress (GL-12)

As agued by Schoderbek et al (1990, pp 39), feedback is needed for effective control. The final process which involves major feedback constitutes monitoring the progress to ensure that the proposed programme is being implemented as intended in order to realise the objectives of the ICT security management process. The technical department has its role to play, but as pointed out in the preceding section, there is a need to clarify the question of overall ownership of the ICT security problem within the organisation. Moreover, it is important to have also clear roles and responsibilities for each department in the organisation when it comes to the implementation of the ICT security management programme, and consequently redefining the job descriptions of individual staff. This ensures that each department (taking into consideration the multi-dimensional nature of the security problem) and each individual staff member understands their roles and responsibilities when it comes to the implementation of ICT security mechanisms. In this case it will be practical to maintain and monitor the progress of the process.

This process takes us back to the component GL-06 which involves providing an evaluation of an organisation's ICT security management process. It also involves evaluating the realisation of benefits to the business from investment in ICT security. The output of this process becomes input into GL-05 and GL-07 and hence the process continues in another circle.

4.3 Discussion and Conclusion

With reference to the previous chapter on the theoretical foundation of ICT security management, we have made use of theories and concepts discussed there in building the proposed holistic approach for managing ICT security in the organisation. We started by describing the system as a whole, and later on the environment and the sub-systems in the environment, with particular attention being paid to the components that may influence the performance of the proposed approach in the organisation. Finally the sub-systems found in the organisation which may affect the proposed system were also presented. We have in the different steps deployed various properties in the theories in order to deal with the complexities of the ICT security management problem. In order to maintain security as built-in functionality and to deal with the multi-dimensional nature of the security problem in each process the activities are based on the SBC model which, as discussed earlier, we used as a model for viewing the security problem. Our observations, practical experience and analysis of various studies (1-5) have also contributed to proposing some of the activities in the proposed framework. The framework also allows for the collaboration and communication of various stakeholders such as management, legal people, human resource, ICT—technical, application owners and service process owners within the organisation.

In Papers VI and VII we have presented and discussed how most of these processes can be achieved in practice. Figure 4-7 shows that the proposed framework adds to the existing body of knowledge.

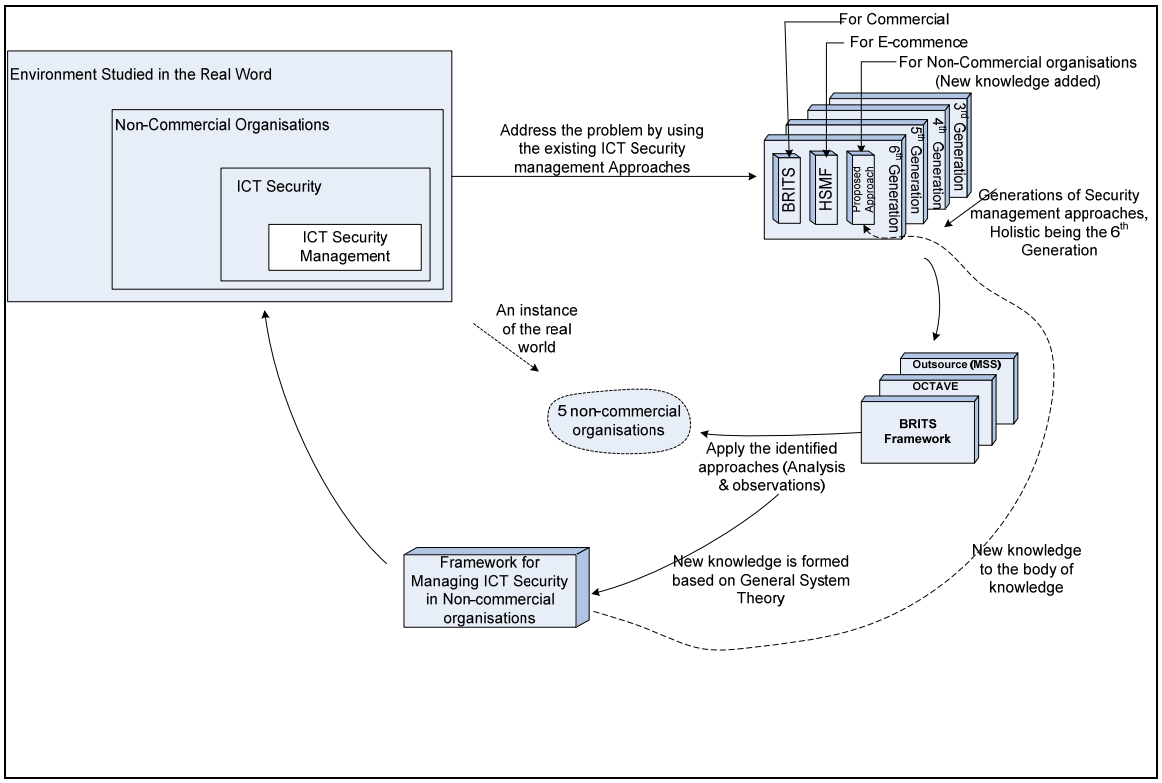
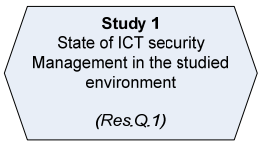


Figure 4-7: New knowledge added to the existing body of knowledge

Chapter 5

5. Summary of the Appended Papers

5.1 Paper I



Res. Q.1: What is the current practice of ICT Security management in organisations in the studied environment? → Indication of the problems

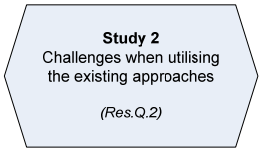
This paper discusses the current state of ICT security management practices in three institutions of higher learning in Tanzania. The three institutions are among the five non-commercial organisations which were involved in the study.

The paper indicated that the complex problem of ICT security has been relegated to the IT department or rather treated as a technical problem, with no relevant organisation-wide ICT security policy. There are obvious gaps at the operational level in each of the studied institutes when measured against existing standards such as ISO 17799, in terms of practices and procedures. For example, all countermeasures lacked documentation, configuration, change management and incident management. In addition, simple measures like data back-up plans, training of end users, etc., are not taking place. No budget was allocated specifically for ICT security. Although the % of computerised core services was found to be less than 50% on average, there was a clear indication that a failure of ICT security could result in substantial adverse consequences.

The paper also indicated that, currently, the necessary infrastructure for digital information security is missing at the national level, i.e. laws, regulations, policies, etc., since a national ICT security policy is non-existent. On the other hand, national traditional policies exist on how to handle critical information securely like hard-copy paper files in the physical world and these are known to all concerned and are being implemented accordingly. In the paper it is argued that, since a new way of handling information is being slowly introduced and implemented, governments in the developing countries, which aspire to acquire and use ICT, should take the initiative in transforming the traditional information security policies into relevant policies to cater for digital information security. Thus, at an organisational level it would be mandatory to acquire, deploy and use ICT in such a way as to guarantee sustainability of the systems and security of the information as per the national ICT security policies.

Finally the paper outlined the likely problems and potential consequences due to ICT risks as the dependency of institutes' core services on ICT grows.

5.2 Paper II

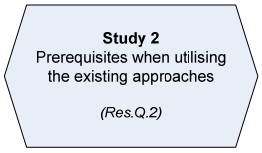


Res. Q.2: What are the prerequisites when utilising the existing ICT security management approaches in attaining a solution to the identified ICT security management problem? → What are the solutions? What are the results when applying them?

This paper attempts to investigate whether ICT risk mitigation can be enhanced using a customised software tool. The Estimated Maximum Information Technology Loss (EMitL) tool was investigated for its suitability as an operational tool for improving ICT risk management. EMitL is a tool utilised in a framework - Business Requirements on Information Technology Security (BRITS) - to bridge the understanding gap between senior management and the technical personnel when it comes to ICT risk management.

The results from this study show that it is possible to customise EMitL into a useful operational tool for interpreting risk exposure due to ICT and suggesting corresponding countermeasures. The study has indicated that the tool could enhance ICT risk mitigation in some ways. One of the problems found in study 1, was the communication gap between the top management and the technical personnel with respect to ICT security problem and their control. The top management could not see the ICT security problem as a business problem, because they looked upon it as a technical one, whereas the technical people needed to understand that ICT security was more than a technical problem (it is more than firewalls, IDS and antivirus!). Using the tool, it was possible to convert financial terminologies mainly financial risk exposure – top management language - to corresponding ICT security terminologies and hence bridge the understanding gap due to the differences in perspective and the language used between the top management and the technical people in an organisation. Using risk information from the top management, the tool generates relevant countermeasures for the environment which would need customisation. Also, at a higher level, the tool helps in giving a rough direction of what needs to be done in order to manage ICT-related risks. This comes out in the form of a Survey Report as described in the paper.
However, the approach depends very much on accuracy in getting the organisation's actual risk exposure at the stage of establishing the potential risk exposure pertaining to that particular organisation. In some cases, the proposed countermeasures did not reflect the organisation's problems. For example, in the dual countermeasures, the generated countermeasure from the tool about mechanical access control suggested automatic gates which are on the advanced side with respect to the current situation of the studied environment. Hence, only through customisation of the tool in that respect could results be arrived at which are relevant to the studied environment. Thirdly, the database engine that contains the countermeasures needs to be updated continuously to reflect the changes in the ICT risk profiles, and so the approach suffers from the same limitations as anti-virus tools.

5.3 Paper III



Res. Q.2: What are the prerequisites when utilising the existing ICT security management approaches in attaining a solution to the identified ICT security management problem? → What are the solutions? What are the results when applying them?

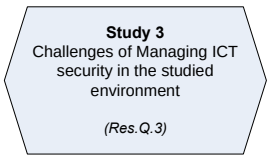
Based on some empirical data, this paper describes typical characteristics of a developing country's ICT environment from an ICT security management point of view. It then discusses the possibility of the environment to benefiting from outsourcing the managed ICT security services approach.

The idea behind outsourcing ICT security is based on the assumption that engaging a managed ICT security provider may be a great relief to such organisations, in that, like insurance, they will be relieved of their ICT security burden by transferring it to a third party. However, the decision to use this kind of approach is never straightforward and is influenced by various constraints when used in the studied environment as discussed in the paper.

The paper points out various prerequisites that need to be considered, if the outsourcing approach is to be opted for as a solution for ICT security management in the studied environment. For example, skilled ICT security staff or hired ICT security experts are required to assist the management in the overall analysis before reaching a decision on whether or not to outsource. This capability is low both within the organisations studied and the surrounding environment. Furthermore, the nature of the operation or implementation requires good infrastructure in place whereby a customer can be serviced remotely. Due to poor infrastructure, remote monitoring is expensive, in which case an alternative is for the MSSP to deploy its equipment and staff at the client site which is definitely far too expensive. Another problem is that of carrying out such MSS operations in the absence of a legal framework that supports the ICT.

We established that, before organisations outsource their ICT security services, they first need to become experts in their ICT-related risks, and they need to see the ICT security problem as a 'white box', a capability that is not available at the moment in the studied environment. This brought us to the conclusion that, because of the perception problem, the low level of awareness of the ICT security problem, and inadequately trained or supervised staff, as observed and discussed in other studies, the situation cannot merely be addressed by simply outsourcing security solutions to the MSSP.

5.4 Paper IV



Res. Q.3: What are the issues and challenges to be addressed in the initial stages of computerisation, from an ICT security point of view?

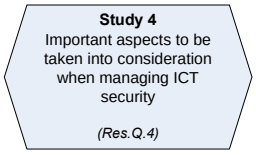
By taking an example of e-government information systems, the paper attempts to highlight and discuss the issues and challenges to be addressed in e-government from an Information Security point of view. Some understanding as to the nature and characteristics of ICT security and associated management techniques is required, in order for e-government initiatives to yield the desired results. In addressing the issues and challenges, the paper used a categorisation proposed by Kowalski (1994), which involves: ethical, cultural; legal; administrative and managerial; operational procedures; policy and technical issues.

The first observation made in the paper indicates that, given the stage at which most developing countries are with respect to e-government development (early stages), they stand a good chance of building in security as they develop their e-government systems. Hence knowing and acknowledging the problem from the beginning might help in developing secure e-government systems which in turn would avail the desired flexibility, efficiency, trust, and effectiveness in government services.

The paper discussed at some length ICT security issues that need immediate attention for e-government systems implementation. The issues discussed underlined the opportunities and fundamental aspects that the studied environment has to address in their initial planning and strategies for ICT. These included well planned ICT security awareness and training programmes, updating the legal framework to incorporate ICT issues, addressing the existing perception gap as detailed in study I and having in place prepared ICT infrastructure.

This paper also highlighted likely areas for further research cooperation between Europe and Africa.

5.5 Paper V



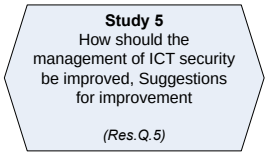
Res. Q.4: What are the important aspects to be taken into consideration in order to successfully manage ICT security? → Given a developing environment with respect to ICT what else need to be observed?

This paper attempted to address the human dimension as an important aspect in the process of attaining, developing, implementing and managing ICT security in organisations or a nation by reviewing and discussing varying aspects related to building a security culture. Security culture encompasses all socio-cultural measures that complement technical security measures. In connection with this, issues of attitudes, behaviour, actions, and motivation as they relate to security have been analysed using concepts from the field of organisational behaviour.

An organisational framework portraying components of a supposedly secure ICT environment in an organisation has been outlined and discussed. The roles of awareness and knowledge of, and skills in ICT security issues which contribute to a culture of security have been emphasised in the discussion and this was further supported by analysis of some data collected from primary research conducted in Tanzania. The findings indicated that there were only 3 courses or modules bearing on ICT security issues among the wide range of IT courses offered in the 6 surveyed institutions. Lack of personnel and resources to support information security education at colleges and universities, was seen as one possible reason why competency in, and awareness of, security issues is relatively low.

In conclusion, the following was found to be apparent—cultivating an ICT security culture was found to be neither simple nor straightforward and is not an issue that can be addressed entirely by organisations alone. There are many factors outside the scope of an organisation that have to be considered. For example, when the focus is on awareness of and training in ICT security, then many aspects would be touched upon, such as the overall education system of a country and other structures supporting it. For education and training to ensure sustainable development, it must be responsive to the needs of society, to technological progress and globalisation trends. The design of training programmes must therefore evolve over time to reflect contemporary demands and must be based on thorough and proper training needs assessment. Thus it is difficult for an organisation to maintain a sound ICT security culture within its environment while its surrounding environment does not. This is because an organisation interacts with other external parties such as suppliers, customers, and business partners. Hence approaches taken at the national level would tend to be more effective as this would make it possible to achieve a common ICT security culture. This paper has tried to shed some light on this and it is an area that calls for further investigation if the goals such as those stipulated in the OECD guidelines—towards the culture of security - are to be realised in practice.

5.6 Paper VI



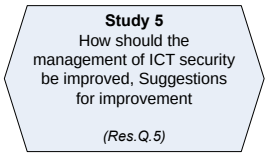
Res. Q.5: How should the management of ICT security in the organisations be improved, in order to reduce the potential financial damage as a result of computerisation?

One of the major problems that were identified and confirmed in the first study was the existence of the problem of perception, in that the general management and general staff perceived ICT security to be a technical problem and not a business problem. Our main assumption then was that, if we are to improve the management of ICT security in the organisation, we needed to address this perception problem first.

The paper outlines a successful mission of how to bridge the perception gap between general management and technicians.

Our objective to bridge the perception gap between the general management and the technical department was achieved through the ten steps, presented in this paper. The paper highlighted the motivation and practical experiences of each step. These included: the CEO buying into the idea first; recognising that the technical departments are the custodians of ICT in the organisation; starting it as a special project; showing where the risks and their consequences are; getting the entire management's attention; taking stock of the existing situation; conducting awareness-raising sessions to address the ICT security problem with respect to the organisation's specific environment; carrying out detailed risk assessment; working out a short-term plan for issues that need immediate attention and a long-term plan to finally develop the countermeasures for the identified problems. The study confirmed that the success of the ICT security management process begins with the management realising the importance of ICT security management. That implies that the management allows the organisation, through its own acquired knowledge and confidence, to internalise the practices, thus enabling people to act confidently at all levels. Knowing about the ICT risks and their consequences for the core service operations of the organisation, the management is more likely to offer its support for ICT security endeavours. Likewise, the technical department, following the support from the management, can address the ICT security problem more holistically in collaboration with other departments, by taking into consideration the non-technical dimensions as well. This was made possible by extending the concept of how ICT security was perceived by staff in the various departments or specialities within the organisation which included corporate lawyers, human resource, technical, accountants, auditors, operations, etc.

5.7 Paper VII



Res. Q.5: How should the management of ICT security in the organisations be improved, in order to reduce the potential financial damage as a result of computerisation?

As pointed out earlier, organisation (Y) was in the process of migrating from proprietary systems to open, inter-operable platforms with TCP/IP as the foundation. This increased the organisation's exposure to ICT security problems. In particular these were the major problems found: a) the existing ICT security policy was outdated, not enforced and lacked any reference to appropriate security services and mechanisms, and so the few existing security mechanisms were only put in place on an ad-hoc basis; b) the lack of clearly defined ICT security responsibilities as such no body was accountable in case of a problem; c) poor documentation, classification and control of ICT assets (hardware, software, information), d) the lack of business continuity plans; and e) the lack of procedures on how to handle ICT assets. Hence there was an immediate need to improve the management of ICT security in the organisation to control the ICT security problems.

In the course of the study, we were able to establish that one of the major causes of these problems was the inadequate operationalisation of the ICT security policy, services and mechanisms in the ICT security management process. Although the policy was there and ICT security control mechanisms were installed/implemented, there was no correlation between the implemented controls/mechanisms and the contents of the policy. In other words, the decision to implement a particular ICT security control was not always based on what is in the policy but rather on the apparent need for it.

This paper attempted to capture the practical experience we encountered in our endeavour to operationalise the ICT security policy, services and mechanisms in the said organisation. In the proposed framework this problem is addressed in process (GL-11) as presented in chapter 4.

Our objective to operationalise the ICT security policy, services and mechanisms in the studied organisation was achieved through a number of steps. These included: mapping the corporate policy to relevant security services, mechanisms and resources; conducting awareness-raising sessions for the general management as well as for the general staff; establishment of an ICT steering committee to oversee and maintain the operationalisation process; redefining and revisiting the departmental responsibilities including individual job descriptions; providing specialised training; restructuring some departments; and clearly defining and placing the overall ownership and authority of the ICT security function in the organisation. We found out that, by intentionally following this path, the operationalisation of the ICT security policy, services and mechanisms becomes an internalised and continuous process which will support the entire organisation in present and future endeavours.

Chapter 6

6. Concluding Remarks

The objective of this research was to suggest ways on how the management of ICT security can be improved in order to reduce the potential financial damage as a result of computerisation in non-commercial organisations, with Tanzania being taken as the case study.

It was not a straightforward undertaking to carry out this type of research in a least developed country, given the limited resources which are being competed for to meet several other basic and important needs. Other constraints included lack of reliable communication and power infrastructure, inadequate ICT project planning, hostile culture towards technology, lack of awareness and the perception that ICT security is a technical issue. However, our objective to address the research problem and meet the intended goals was achieved through a number of stages:

- First we were able to carry out an investigation of the current practice of ICT security management. The results of the investigation gave us an indication of the magnitude of the ICT security problem in the studied environment;
- The following stage was to review the existing ICT security for management approaches to determine whether there is a suitable ICT security management approach for the identified problem. During the review, three ICT security management approaches namely BRITS framework, OCTAVE and Outsourcing, were identified as possible candidates for addressing the problem. These approaches were then tested at different stages of the research to determine their suitability for addressing the ICT security management problem in the studied environment;
- The initial findings of the research showed that the studied organisations and the environment were in the initial stages of computerisation. The following stage therefore focused on an investigation of the issues and challenges to be addressed in the initial stages of computerisation, from an ICT security point of view, particularly in the developing country environment;
- Given the developing environment with respect to ICT, we were also motivated to investigate the important aspects to be taken into considerations in order to successfully manage ICT security in the environment; and finally
- We were able to develop and suggest ways for addressing the observed ICT security management problem, by proposing a holistic approach.

We achieved our goal as stated in section 1.3, by proposing a holistic approach that would improve the ICT security management process in the organisation. In particular the proposed approach intends to reduce the complexity of dealing with the ICT

security management problem and addresses the perception gap between the general management and technicians. Furthermore, it acts as a guide to the management in the process of introducing ICT security management and maintains its operationalisation continuously throughout the organisation.

In the following section, we investigate the validity of our work. After we have argued for the validity, we shall then present what we perceive to be the contribution of this research. We shall then conclude our remarks by briefly discussing the practical implications of this research work and making recommendations for future work as a result of this research.

6.1 Quality, Validation and Limitation of the main Research work

To support the validity of this research, five case studies were conducted. The studies and their contributions are described and presented in nine (9) published papers, of which seven are appended to this thesis.

The second approach to show the validity of our work, which used the qualitative approach, is to make use of the four criteria proposed by Lincoln and Guba (1985) to assess validity. These are credibility, transferability, dependability and confirmability. Credibility is an evaluation of whether or not the research findings represent a credible conceptual interpretation of the data drawn from the field. Transferability is the degree to which the findings of the inquiry can apply or be transferred beyond the bounds of the context of the study. This means demonstrating the applicability of the results of the study in one context to other contexts. Dependability is an assessment of the quality of the integrated processes of data collection, data analysis and theory generation. And confirmability is a measure of how well the inquiry's findings are supported by the data collected (Lincoln and Guba; 1985). In the next section, we discuss how each of these criteria was applied to our work.

(a) **Credibility**: Our research was basically dealing with people, which means social reality is implied. Social reality is something that is constantly changing and multiple perspectives are often involved which lead to multiple realities. In our work, we addressed this problem by fixing our viewpoint and setting the boundary of the study so that it is possible to establish realities concerning the phenomenon in focus. Furthermore, the methods used at various stages of the work have been used in similar studies conducted elsewhere as detailed in the research methodology section. In this case subjectivity on the part of the researcher as a result of influences such as past knowledge was minimised.

(b) **Transferability:** Although we limited ourselves to five organisations in Tanzania, so that we could establish the reality concerning the phenomenon in focus, we have tried to make our solution to the problems as general as possible. Thus we believe that the results obtained here are a true

reflection of the studied phenomenon which may prove to be of value and useful in other similar[44] situations.

(c) **Dependability**: Our research was a qualitative one, and by their nature qualitative studies cannot be replicated due to changing realities. Therefore what is important is to emphasise the stability and consistency of the enquiry process. In our study we ensured that the processes used in the enquiry are consistent.

(d) **Confirmability**: Throughout the research process, we ensured that the types of data collected and the assumptions we have made are those defined within the design approach and those which have relevance to the phenomenon in focus.

6.2 Contributions

Reflecting on the problem and the purpose of the research, the main contributions of this research can be summarised as follows:

(i) The main contribution is to the body of knowledge achieved through the proposed holistic approach for managing ICT security in non-commercial organisations. Figure 6-1 summarises the proposed approach.

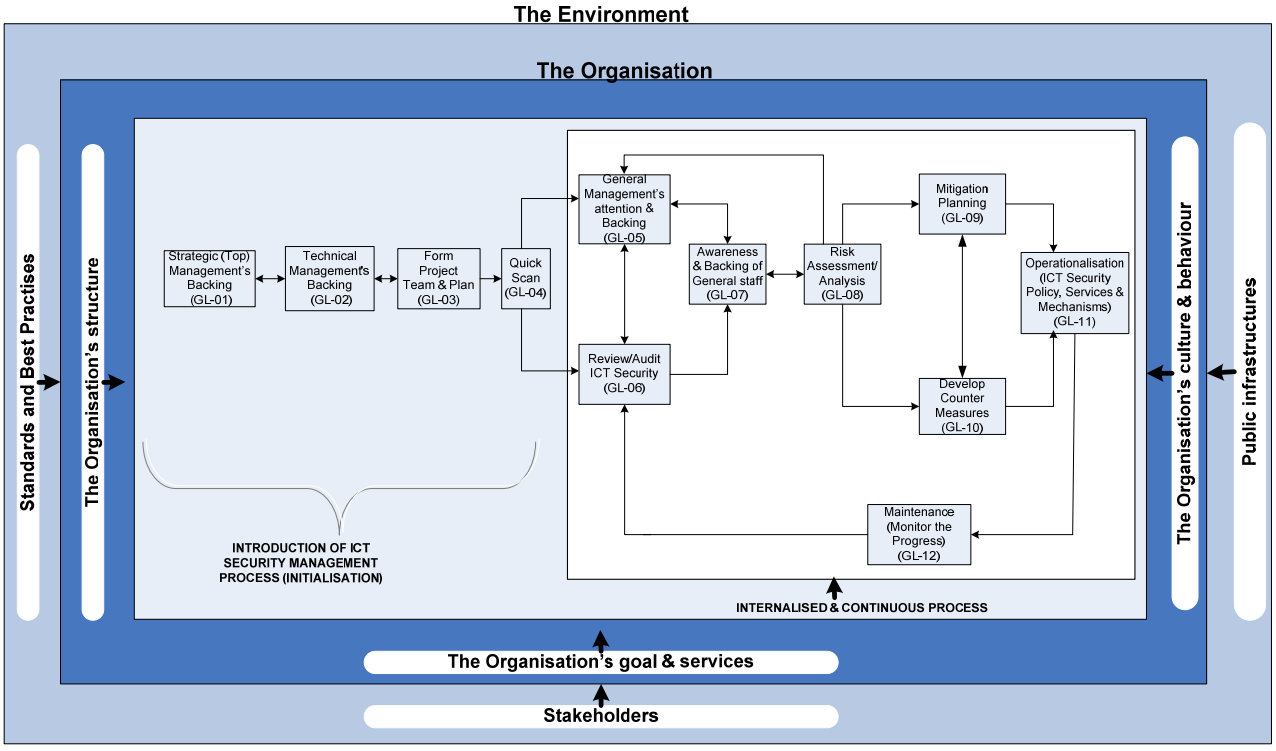


Figure 6-1: Proposed Framework for Managing ICT Security in Non-Commercial Organisation

[44] Similar situation here refers to Least Developed Countries, mostly in sub-Saharan Africa, which according to (Gelan, 2006), are characterised as low-income countries suffering from long-term constraints against growth. In particular, these growth constraints include low level of human resource development, and severe structural weaknesses in the economic, social, and political realms.

General Systems Theory is the main foundation of the approach, which addresses the ICT security management problem among other things in the following ways:

(a) Complexity – the proposed approach has significantly reduced the complexity by use of the guidelines;
(b) Changeability – by providing repetitiveness and an explicit management process for the maintenance of ICT security;
(c) Conformity – with the holistic approach;
(d) Interdisciplinary – Draws upon different disciplines from different departments to address the security problem, thereby addressing the perception problem;
(e) Awareness and execution ability – leads to backing of senior management, general management and staff. This was found to be essential as is the fact of defining the true overall ownership of the ICT security management process within the organisation. Staff become aware and execute their different responsibilities; and
(f) Continuity – Once introduced it becomes internalised and a continuous process through operationalisation of the ICT security policy, services and mechanisms.

See chapter 4 for more details on the different parts of the approach and its deployment in case studies in PAPER VI & VII. This relates to the main research question.

(ii) Contribution to the body of knowledge with respect to the validation of the applicability of one of the typical ICT security management approaches - the BRITS framework - to the identified ICT security management problem in non-commercial organisations [PAPER II]. Furthermore in a different study [PAPER III], an analysis of the applicability of OUTSOURCING as one of the ICT security management approaches was conducted. Both contributions relate to research question 2.

(iii) Contribution to increased empirical knowledge on the aspect of the importance of the holistic ICT security management process, particularly in bringing together staff from various departments or specialities to enable them to discuss and reach a consensus on how to address ICT security management in the organisation. We found that this process makes it possible for the organisation, through its own acquired knowledge and confidence, to internalise the ICT security management practices, thus enabling people to act confidently at all levels. This helps the ICT security management process to be a living process in the organisation. This relates to the main research question or question 5. [PAPER VI & VII]

(iv) Contribution to the body of empirical knowledge on the issues and challenges when managing ICT security in the developing world. The issues discussed underlined the opportunities and fundamental aspects that the studied environment has to address in their initial planning and strategies for ICT. These included what kind of parameters or structures should be included in the environment and how they should be adjusted for optimal results, which can

lead to a better performance of the systems implemented in the organisations. This relates to research question 3 [PAPER IV].

(v) Contribution to raising the level of ICT security awareness particularly of managers in the studied environment. During the research fieldwork in Tanzania, more than nine (9) ICT security seminars and public lectures which involved more than 1,000 participants in total were conducted.

6.3 Practical Implications

The study of ICT security management is wide and is applicable to all types of organisations worldwide. Our intention in the research work was to assess the current state of ICT security management and uncover the likely problems and potential consequences arising from ICT risks, and hence capture top management's attention about the problem of ICT security in their organisations. Therefore the usefulness and quality of this work can best be judged from a senior management perspective.

Practitioners – e.g. senior management, ICT security managers, financial managers, Human resources managers, Auditors, Corporate lawyers, consultants in the studied environment – need an ICT security management approach that can help and guide them to introduce and maintain an appropriate level of ICT security in their organisation. We believe that the proposed approach, which is based on the empirical reality in which the practitioners are situated, is ideal for addressing the ICT security management problem as observed in the research. This approach acts as a guideline for ICT security management and therefore practitioners can use it straightaway.

Governments can use the results to create the environment for an improved ICT security management process in organisations. This may include the introduction or enhancement of various standards and best practices, legislations and various infrastructures.

6.4 Recommendations for future work

We have some recommendation to make regarding future work. First, we have attempted in practice to use part of the proposed holistic approach as detailed in (PAPER VI and VII) to indicate its validity. In order to allow a generalisation, it would be interesting to see the results of using the proposed framework in other organisations, in the government and in different environments as well. One future research activity could include how to adjust the parameters in the framework's environment for optimal results of the ICT security management process in the organisations.

Secondly, in our work with reference to the studied environment and throughout the literature review, the effect of culture, for example, on the question of accountability seems to be one of the major challenges to deal with in the overall management of ICT security. Further research focusing on this area could yield, among other things, a better understanding of the environment and consequently an improvement of the proposed holistic approach.

Thirdly, there is the question of islands of information systems as observed in the study. Probably this state of islands of information systems can be seen today as a protection mechanism or strategy when dealing with security in such an environment. This means providing inter-operability while preserving each separate system's identity. It will therefore be interesting to see how the proposed framework performs in an inter-operability situation, particularly when handling organisations or government institutions with different security maturity levels, within the same environment and outside the environment. Will this be a problem in the future or a challenge to find other solutions? It will also be interesting to see the drawbacks or limitations of interoperability from security point of view.

Fourthly, following the findings from the use of the EMitL tool during the research, the most obvious direction for further work is the improvement of the tool's database. EMitL was first released in 1996 and updated in 1999. ICT security is a moving target. Threats, organisational needs, and technologies change constantly. Ongoing improvements to the database (security measures, practices, and technology) are necessary to keep up to date with potential attackers and to keep abreast of the organisation's service needs. The improvement could also include updating some countermeasures that currently address specifically Swedish organisations to more generic countermeasures which would be relevant to the developing world as well. Although it is not a complicated system, the lack of an operating manual could render it difficult for users to successfully use it, particularly in the environment under discussion. The improvement could therefore include writing a general user manual.

References

Alberts, C. & Dorofee, A. (2003) *Managing Information Security Risks, the OCTAVE Approach.* Addison Wesley.

Allen, J., Gabbard, D., & Christopher (2003) *Outsourcing Managed Security Services* Website, URL: http://www.cert.org/security-improvement/modules/omss/index.html (Accessed on 15th April, 2005)

Anderson, R. (2001) *Why Information Security is Hard – An Economic Perspective*, University of Cambridge Computer Laboratory. Also available at Website, URL: http://www.acsac.org/2001/papers/110.pdf (Accessed on 5th May, 2005)

Bakari, J. K. & Mboma, L. (2001) *The current status of ICT at the University of Dar es Salaam*. Status Report, Directorate of Planning and Development (DPD), University of Dar es Salaam.

Bakari, J. K. (2005) *Towards A Holistic Approach for Managing ICT Security in Developing Countries: A Case Study of Tanzania*. Licentiate Thesis. Report Series No. 05-011. Department of Computer and Systems Science, Stockholm University.

Bakari, J. K., C. Yngström, L., Magnusson, C., Chaula, J. (2004) *Towards Managing ICT Security in Non-Commercial Organisations in Developing Countries* Proceedings of Information Security South Africa (ISSA), enabling tomorrow Conference, eds. Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM, Midrand, Johannesburg, South Africa, June 30 - July 02, 2004.

Baskerville, R. (1988) *Designing Information System security*. John Wiley Information Systems Series.

Benno, J. (2002) *Why the use of ICT engenders Legal Problems – in search of a common Denominator*. in Seipel, P. (2002) Law and Information Technology Swedish View' Swedish ICT Commission, An anthology produced by the IT Law Observatory of the Swedish ICT Commission, Information and Communication Technology Commission Report, Stockholm 2002, STATENS OFFENTLIGA, UTREDNINGAR, Swedish Government Official Reports, SOU 2002:112.

Bertalanffy, V. L. (1950) *An outline of General Systems Theory*. The British Journal for the Philosophy of Science, (Aug., 1950), Vol. 1, No. 2, pp. 134-165.

Bertalanffy, V. L. (1968) *General Systems Theory: Foundation, Development, Application.* George Braziller, Inc. New York.

Bertalanffy, V. L. (1972) *The History and Status of General Systems Theory*. The Academy of Management Journal, General Systems Theory, (Dec., 1972), Vol. 15, No. 4, pp. 407-426.

Bhattarakosol, P. (2003) *IT Direction in Thailand, Cultivating an E-Societ*y. IT Pro September/October 2003: Paper Published by the IEEE Computer Society, pp. 16-20.

Bishop, M. (2003) *Computer Security, Art and Science*. Addison Wesley.

Bjorck, J. F. (2001) *Security Scandinavian Style, Interpreting the Practice of Managing Information Security in Organisations*. Licentiate Thesis. Report Series No. 01-017. Department of Computer and Systems Science, Stockholm University.

Bjorck, J. F. (2005) *Discovering Information Security Management*. PhD Thesis. Report Series No. 05-010. Department of Computer and Systems Science, Stockholm University.

Blakley, B., McDermott, E. & Geer, D. (2001) *Information Security is Information Risk Management*. Proceedings of the workshop on New security paradigms, September 2001. ACM Press New York, NY, USA.

Caelli, W., Longley, D & Michael Shain, M. (1991) *Information Security Handbook*. Macmillan Publisher Ltd.

Caralli, A. R. (2004) Also contributed by Allen, H. J., Stevens, F. J., Willke, J. B., and Wilson, R. W. *Managing for Enterprise Security. Networked Systems Survivability Program*, Technical Note CMU/SEI-2004-TN-046, Carnegie Mellon University, USA.

Casmir, R. & Yngström, L. (2003) *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.

CC (2005) Website, URL: http://csrc.nist.gov/cc/Guidance.html, (Accessed on April, 2005).

CC (2006) *Introduction to Common Criteria*, Website, URL: http://www.cesg.gov.uk/site/iacs/itsec/media/intro-guides/criteria.pdf, (Accessed on 20th November, 2006).

Cert (2003) *CERT/CC Overview Incident and Vulnerability Trends*. Web site, URL: http://www.cert.org/present/cert-overview-trends/module-2.pdf, CERT® is a registered service mark of Carnegie Mellon University. (Accessed on 15th April, 2005).

Cert (2005) Website, URL: http://www.cert.org/stats/cert_stats.html#incidents (Accessed on 25th February, 2005).

Chacha, M. K. L. (2000) *The impact of Information Technology on Internal Auditing in Tanzanian Organisations*. Master of Business Administration thesis. University of Dar es Salaam.

Chaula, A. J. (2006) *A Social-Technical Analysis of Information Systems Security Assurance, A Case Study for Effective Assurance*. Ph.D Thesis. Report Series No. 06-016. Department of Computer and Systems Science, Stockholm University.

Cia (2005) World facts book, Website, URL: http://www.cia.gov/cia/publications/factbook/fields/2116.html (Accessed on 19th January, 2005).

Creswell, J. W. (1998) *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Sage Publications, London, New Delhi.

Davison, R.M. (1998) *An Action Research Perspective of Group Support Systems: How to Improve Meetings in Hong Kong*. PhD Thesis, Department of Information Systems, City University of Hong Kong: Website, URL: http://www.is.cityu.edu.hk/staff/isrobert/phd/phd.htm., 1998. (Accessed on 15th November, 2006).

Dimopoulos, V. & Furnell, F. (2005) *A protection Profiles Approach to Risk Analysis for Small and Medium Enterprises*. IFIP TC-11.1 & WG 11.5 Joint Working Conference, USA: Springer pp. 267-283.

Drew, P. E. & Foster, G. F. (1994) *Information Technology for selected countries. Reports from Ireland, Ethiopia, Nigeria, and Tanzania*. The United Nations University, UNUP-831.

Drucker, P (1993) *Management Challenges for the 21st Century*, Harpers Business

EC46 (1995) DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995.

Eloff, M. M. & Eloff, J.H.P. (2003) *Information Security Management System: Processes and Products*. IFIP TC11 18th International Conference on Information Security (SEC2003) May 26-28, 2003, Athens, Greece.

Eloff, M. M. & Eloff, J.H.P. (2003) *Information Security Management – A new Paradigm*. Proceedings of SAICSIT 2003, pp. 130-136.

Frisinger, A. (2001) *A Generic Security Evaluation Method for Open Distributed Systems*. Ph.D Thesis. Department of Teleinformatics, Royal Institute of Technology, Sweden.

Furberg, P. (2002) *Law making and IT: Reflection on the need for new Concepts and Categories of Thoughts* - in Seipel, P. (2002) Law and Information Technology Swedish View' Swedish ICT Commission. An anthology produced by the IT Law Observatory of the Swedish ICT Commission, Information and Communication Technology Commission Report, Stockholm 2002, STATENS OFFENTLIGA, UTREDNINGAR, Swedish Government Official Reports, SOU 2002:112.

Gelan, K. M. (2006) *A Theoretical Model for Telemedicine: Social and Value Outcomes in Sub-Sahara Africa*. Ph.D Thesis. Report Series No. 06-020.Department of Computer and Systems Science, Stockholm University.

Gerber, R. (2003) *Research Method, 'An Overview of some research methods'* Website, URL: http://www.petech.ac.za/robert/resmeth.htm (Accessed on 23rd November, 2003).

Gordon, L. A., Loeb, P. M., Lucyshyn, W. & Richardson, R. (2006) *2006 CSI/FBI Computer Crime and Security Survey*. Computer Security Journal; Volume XXII, Number 3.

Granger, S. (2001) *Social Security Engineering Fundamentals* Website, URL: http://www.securityfocus.com/infocus/ (Accessed 15th January, 2005)

Hill (2005) *Disaster Recovery Planning: Conducting a Risk Analysis*. Web site, URL: http://www.hill.com/archive/pub/papers/2003/11/paper.pdf (Accessed on 29th March, 2005)

Hong, K., Chi, Y., Chao, R. L & Tang, J. (2003) *An integrated system theory of information security management*. Information and Management & Computer Security 11/5, 2003, Page 243-248.

IBM (2004) IBM Website URL: http://www.ibm.com/ (Accessed on 15th January, 2004)

ISACA (2005) Website, URL: http://www.isaca.org, (Accessed on April, 2005).

ISMS (2004) The ISMS International User group (IUG) Journal, Issues 5, November 2004. Also available at Website URL: http://www.xisec.com/Issue5.pdf (Accessed on March, 2007).

ISO/IECFAQ (2002) International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, Frequently Asked Questions. Website, URL: http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf (Accessed on June 2004)

ISO-7498 (ISO 7498-2-1988(E) Security Architecture Framework.

ITGI (2006) *IT Control Objectives For Sarbanes-Oxley, The role of IT in the Design and Implementation of Internal Control Over Financial Reporting*. 2nd Edition, September 2006, IT Governance Institute (ITGI)

ITIL (2005) Website, URL: http://www.itil.org.uk/ (Accessed on April, 2005)

itSMF (2006) *Aligning COBIT, ITIL and ISO 17799 for Business Benefit.* The IT Service Management Forum. Website, URL: https://www.isaca.org/Template.cfm?Section=Downloads3&CONTENTID=22490&TEMPLATE=/ContentManagement/ContentDisplay.cfm, (Accessed on January, 2007)

Kaplan & Norton (1990) *The balanced score card* Website, URL: http://www.balancedscorecard.org/ (Accessed on October 9th, 2006).

Klijfhout, E. (1996) I*nformation and Communication Technologies in the developing World, The Case of Swaziland*. Ph.D Thesis. Centre for Development Cooperation Services, Vrije Universiteit, Amsterdam.

Kowalski, S. (1994) *IT Insecurity: A Multi-disciplinary Inquiry*. Ph.D Thesis. Report Series No. 94-004. Department of Computer and Systems Sciences, Stockholm University.

KPMG (2002) *East Africa Fraud Survey 2002*. Website, URL: http://www.kpmg.co.ke/ (Accessed on 23rd October, 2003).

Kuhn, T. (1962) *The Structure of Scientific Revolutions*, in Curd, M. & Cover, A. J. (1998) *Philosophy of Science – The Central Issues*. W W Norton & Co Inc.

Kumar, P. (2006) *The Technology Auditor: How Automation Is Changing Auditors' Roles*. Information Systems Control Journal, Volume 5, 2006. Issued by ISACA, pp. 41-42.

Lincoln, Y and Guba, E (1985) *Naturalistic inquiry* Beverly Hills, CA: Sage Publications, Inc.

Lindskog, S. (2000) *Observations on Operating System Security Vulnerabilities*. Licentiate Thesis. Department of Computer Engineering, Chalmers University of Technology.

Looijen, M. (1998) *Information Systems, (Management, Control and Maintenance)*, ISBN: 90-267-2846-8.

Lrct (2005) *Law reform Programme of Tanzania* Website, URL: http://www.lrct-tz.org/publications.html (Accessed on 20th February, 2005).

Magnusson, C. (1999) *Hedging Shareholders Value in an IT dependent Business Society" THE FRAMEWORK BRITS*. Ph.D Thesis. Report Series No. 99-015. Department of Computer and Systems Science, Stockholm University.

Massingue, S. V. (2003) *Building Awareness and Supporting African Universities in ICT Management, THE BIG ICT FIVE (Strategy, Development/Acquisition, Implementation, Utilisation, Service Management)*. Ph.D Thesis. Delft University of Technology.

Mbwette, T.S.A and Mboma, L. (2000) *The Importance of a common Strategy of Information and Communication Technology (ICT) Applications in Tanzanian Universities and other Institutions of Higher Education* Proceedings of a workshop, University of Dar es Salaam.

MEA (2001) *A Country ICT Survey for Tanzania*. Final Report, Prepared for SIDA, Esselaar, Miller and Associates, November, 2001.

Mhayaya, G. S. (2003) *A study of the potential usage of ICT (E-government) in improving efficiency and effectiveness of 'executive functions' of the government including delivery of Public Services, Case of Tanzania*. Master of Engineering Management thesis. University of Dar es Salaam.

Moyo, L. 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, ISSN: 0268-1102 JRNL CODE: ITFD.

Myers, M. D. (1997) *Qualitative Research in Information Systems*. MIS Quarterly (21:2), June 1997, pp. 241-242. *MISQ Discovery*, archival version, Website, URL: http://www.misq.org/discovery/MISQD_isworld/. (Accessed on 15th November, 2006).

Myers, M. D. (1999) *Investigating Information Systems With, Ethnographic Research.* Communications of the Association for Information Systems, Volume 2, Article 23.

O'Connor, T. (2004) *Research methods, Survey research design* Website, URL: http://faculty.ncwc.edu/TOConnor/308/308lect07.htm. (Accessed on 15th November, 2006).

Odedra, M. & Madon, S. (1993) *Information Technology Policies and Application in the Commonwealth Developing Countries*. A Commonwealth Secretarial Publication, ISBN 0 85092 401 4.

OECD (2006) *OECD Studies in Risk Management, Norway INFORMATION SECURITY ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT*.

Website, URL: http://www.oecd.org/dataoecd/36/16/36100106.pdf. (Accessed on 21st November, 2006).

Peltier, R. T. (2002) *Information Security Policies, Procedures, and Standards, Guidelines for Effective Information Security Management*. AUERBACH.

Pfleeger, P. C. & Pfleeger, L. S. (2003) *Security in Computing* Third Edition, PRENTICE HALL PTR.

Posthumus, S. & Solms, V. R. (2004) *A framework for the governance of information security*. Journal of Computers & Security (2004), ELSEVIER Ltd., Vol. 23, pp. 638-646.

Purser, A. S. (2004) *Improving the ROI of the security management process*. Journal of Computers & Security, Vol.23 pp. 542-546.

Rapoport, R. N. (1970) *Three Dilemmas in Action Research Human Relations*, (23:4), 1970, pp. 499-513.

Robbins, P. S. (2003) *Essentials of Organisational Behaviour*. Pearson Education, Prentice Hall.

Robson, C. (2002) R*eal World Research, A Resource for Social Scientists and Practitioner-Researchers* Second edition, Blackwell Publishing.

Schneier, B. (2004) *Security and Compliance* Published By The IEEE Computer Society, IEEE Security & Privacy July/August 2004, pp. 96,

Schoderbek, P. P., Schoderbek, G. C. & Kefalas, G. A. (1985) *Management Systems, Conceptual Considerations.* Third Edition, Business Publications, Inc. Plano, Texas 75075.

Schoderbek, P. P., Schoderbek, G. C. & Kefalas, G. A. (1990) *Management Systems, Conceptual Considerations*. Custom Edition, Irwin, Boston, 1990, The McGraw-Hill companies.

Sadowsky, G., Dempsey, J. X., Greenberg, A., Barbara J. M. & Alan Schwartz, A. (2003). *Information Technology Security Handbook.* Global Information and Communication Technologies Department, The world bank.

Skyttner, L. (2001) *General Systems Theory, Ideas & Application*. World Scientific Publishing Co. Pte. Ltd.

Solms, V. B. & Solms, V. R. (2004) *The 10 deadly sins of information security management*, Journal of Computers & Security, ELSEVIER Ltd., Vol.23 No 5 ISSN 0167 –4048, 2004, pp. 371-376.

Solms, V. B. (2005) *Information Security governance: COBIT or ISO 17799 or both?* ELSEVIER Ltd., Computer & Security, 2005 Vol 24 pp. 99-104.

Straub, D. W., Loch, K.D. and Hill C.E. (2001) *Transfer of Information Technology Developing Countries: A test of Cultural Influence Modelling in Arab World.* Journal of Global Information Management, Vol. 9, No. 4, pp. 6-28.

Sulla, E. (2004) *Performance of Card-Based Payment Systems on Customer Satisfaction in Financial Institutions in Tanzania, Case study of CRDB Bank Ltd*. Master of Business Administration (Finance) thesis. University of Dar es Salaam.

Suluo, S. J. A. (2003) *The role of Information and Communications Technologies in Insurance industry: The case of Tanzanian Insurance Organisations*. Master of Engineering Management thesis. University of Dar es Salaam.

Sulzbeger, H. A. (1947) New York Times, March 1947

Tanzania (2005) *The United Republic of Tanzania*, official website Website, URL: http://www.tanzania.go.tz/ (Accessed on 10th January, 2005)

Tarimo, C. N. (2006) *ICT Security Readiness Checklist for Developing Countries, A Social-Technical Approach*. Ph.D Thesis. Report Series No. 06-017. Department of Computer and Systems Science, Stockholm University.

TRCA (2006) Website, URL: http://www.tcra.go.tz/Market%20info/statsTelecom.htm, (Accessed on 13th September, 2006).

Tsiakis, T. & Stephanides, G. (2005) *The economic approach of information security* Computers & Security, ISSN 0167 –4048, 2005, Vol.24 pp. 104-108.

TzICT (2003), Tanzania National ICT Policy, March, 2003.

Valantin, R. (1996) *Global Program Initiative: Information Policy Research*; In Information Technology for Development v7n2 pp. 95-103 Oct 1996 ISSN: 0268-1102 JRNL CODE: ITFD.

Vision 2025 (1999) *The Tanzania Development Vision 2025*. Planning Commission, Website, URL: http://www.tanzania.go.tz/vision.htm (Accessed on 17th September 2005)

Vroom, C. & Solms, V. R. (2004) *Towards information security behavioural compliance*. Computer & Security (2004) Vol 23, 191-198.

Wanyembi G. & Looijen, M. (2000) *A Model For Improving ICT Management*. Proceedings of the 2000 IEEE International Conference on Management of Innovation and Technology, Singapore, 12-15 November, 2000.

Weinberg, G. (1975) *An Introduction to General Systems Thinking*, John Wiley, New York.

Wilson, M. & Hash, J. (2003) *Building an Information Technology Security Awareness and Training Program*. NIST Special publication 800-50.

Yngström, L. (1996) *A Systemic-Holistic Approach to Academic Programmes in IT Security*. Ph.D Thesis. Report Series No. 96-021. Department of Computer and Systems Science, Stockholm University.

Zuccato, A. (2005) *Holistic Information Security Management Framework*. Ph.D Thesis. Department of Computer Science, Karlstad University, Sweden.

Part II

Publications

State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case study

Reprinted from

The Proceedings of the 5th IEEE International Conference on
Advanced Learning Technologies" (ICALT 2005)
in Kaohsiung, Taiwan
July 5 - 8, 2005
pp. 1007-1011, ISBN 0-7695-2338-2.

State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study

Jabiri Kuwe Bakari[1], Charles N. Tarimo[2], Louise Yngström[3] & Christer Magnusson[4]
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: {si-jba[1], si-cnt[2], louise[3], christer[4]}@dsv.su.se

Abstract

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

This paper discusses the current state of ICT security management practices in three institutions of higher learning in Tanzania. The discussion includes the problems and consequences of ICT risks.

1. Introduction

Information and Communication Technology (ICT) plays an increasingly important role in higher education worldwide. As in the developing countries, where the student population has been growing without a significant increase in other resources, ICT is achieving a breakthrough in the management and teaching of online learning.

Tanzania has not been left out in the utilisation of ICT, Organisations, regardless of their size, acquire/adopt and use the new technology. The significant achievement of ICT in Tanzania can be traced from the early nineties after various adjustments of regulatory and commercial policies, both macroeconomic and within ICT's converging sectors [3, 4]. Since then, Tanzania has experienced dramatic changes in the use of ICT. This usage is coupled with limited knowledge, use of different varieties of software and hardware, poor infrastructure and maintenance of ICT in general [3].

Following the ongoing research study, a discussion on the state of ICT security management practices in three institutes of higher learning in Tanzania is presented. Business Requirements on Information Technology Security (BRITS) framework has been used to guide the study. The framework is a systemic-holistic approach to multi-disciplinary problems which combines finance, risk transfer, IT and security in a coherent system [2]. BRITS can be used to bridge the gap between the top management and IT personnel when it comes to risk management in organisations.

This study had two primary goals: firstly to assess the current state of ICT security management, mainly with respect to ICT security strategies, policies and their implementation, as well as operational issues. Secondly, to uncover the likely problems and potential consequences due to ICT risks as the dependency of institutes' core services on ICT grows.

2. The studied institutes

Three institutes of higher learning were identified for the study. By virtue of being higher learning institutes, the way they deploy, secure, use and manage ICT in general and ICT security in particular, presents a fair representation of the state of ICT security management in other institutes and organisations of a similar set-up in the country. The random selection method was used to get the three institutes from among other institutions. There was no reason for mentioning the names of the studied institutions. Our interest was to study the state of ICT security management hence the studied institutes are referred to as **X**, **Z**, and **V** throughout the paper.

Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)
0-7695-2338-2/05 $20.00 © 2005 **IEEE**

Institute **X** has approximately 1700 staff (academic and administrative) and a student population of approximately 14,000 (undergraduate and postgraduate). The utilisation of ICT at institute **X** can be traced from 1995, when the ICT strategic plan was put in place for the first time. The institute has more than 2000 personal computers (PCs) of which more than 95% are connected to the network, and probably the best network infrastructure in the country. A substantial number of functions of the core services have been and still are in the process of being computerised.

Institute **Z** conducts its operations (distance learning) through regional and study centres. Currently there are 23 regional centres and 69 study centres throughout the country, with approximately 371 staff (academic and administrative) and a student population of more than 16,000. The institute has approximately 112 PCs with 71 PCs networked in a small LAN at its head office. A very small part of the institute's core services are computerised.

Institute **V** has approximately 300 staff (academic and administrative) and a student population of 1200. The institute has a back-bone infrastructure made up of fibre optic double rings and wireless, which has about 32 access points as back-up. This means each department has a LAN, which is reachable by physical cable and wireless. The institute has approximately 200 PCs of which 80% are connected to the institute's network. We learned also during the study that approximately 200 more PCs will be added in about three months time.

3. Methodology

Qualitative method approach was used where four types of questionnaires adopted from [1] and [2], were prepared as follows; the first one was addressed to the top management (strategic), the second one to the operational management (operational), the third one to the technical department (operational, procedures and implementation) and the fourth one to general staff (implementation/practice).

A pilot study was conducted between mid-August and October 2004. The results of which led to face-to-face interviews during December 2004 – January 2005, with selected respondents—mainly the top management, chief financial officers, operational managers, IT directors, system administrators and general staff. The results of the study are presented next.

4. State of ICT security management

We briefly present the study findings here, first the percentage dependence of core services (Core Sev.) on ICT. Then counter-measures that are in place in each of the studied organisations are presented under the following categories of ICT security controls: Organisational and management; technical; and physical and environmental.

Figure 1 presents percentage of computerised core services functions.

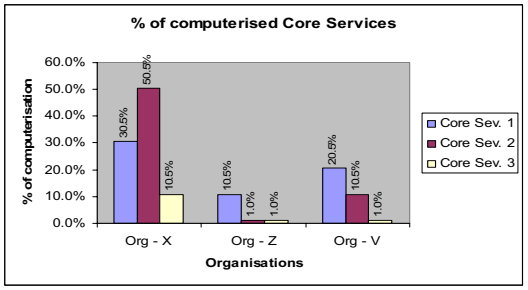


Figure 1: % of computerised core services

Although the percentages of dependency indicated in the figure 1 are less than 50% on average, a failure of the ICT could result into substantial adverse consequences.

4.1 Organisational and Management Controls

4.1.1. Institute X. The current ICT policy plan of the institute is outdated but plans are underway to review it. ICT security features in the institute's strategic plan. However, an ICT security policy is non-existent. It is expected that the review process will involve the development of an ICT security policy. The study indicated that information security awareness & training programs, and periodic reminders are only given to staff members when an incident of insecurity has occurred.

The respondents at the operational management level have a feeling that the rules, procedures and practices are fragmented because of the absence of ICT security policy and its enforcement. There are only un-coordinated initiatives at individual and departmental level. Approximately 3.2% of the total budget is allocated to ICT activities. However, almost 50% of the allocated budget is used for salaries and about 25% is used for Internet connectivity charges. This leaves only 25% which is about 0.75% of the institute's total budget for other ICT related activities like gateway services, websites, purchasing new PCs, software and maintenance. There is no specific budget allocated for

ICT security. There exist ad-hoc measures where some ICT security related activities are executed, like purchasing security related products (e.g. anti-virus, firewalls, and switches for building VLANs etc.) and training, but all these are predominantly donor-funded and are not coordinated.

4.1.2. Institute Z. The level of computerisation in the institute is very low compared with the other two institutes. The institute has just concluded its ICT strategic plan, which indicates that there will be a very high degree of dependence on ICT in the near future. The plan includes ICT policy and master plan. ICT security is well addressed at the strategic level and various institute regulations are being updated to incorporate ICT security. Currently, only 0.5% of the total budget is allocated to ICT activities, mainly for purchasing PCs and to cater for maintenance and Internet charges.

4.1.3. Institute V. The institute is currently in the process of formulating an ICT policy, which involves developing information security policy. The study indicated that information security awareness and training have also just begun with senior management, in parallel with the formulation of the ICT security policy.

The budget allocated for ICT activities is less than 2% of the total budget, mainly to cater for the purchase of the PCs and communication rental charges (before the network was put in place recently, dial-up was the main means of connectivity for all departments). The entire network infrastructure was made possible by donor-funds.

4.2 Technical control

4.2.1. Institute X. The institute has a fairly good network infrastructure in place. There is an indication that VLANs were to be used to separate different user groups for security reasons, but the study has indicated that this measure is not being practised. The same goes for updating operating systems and anti-virus; there are no procedures in place to make sure that they are updated throughout the institute network, unless there are problems reported to the technical department.

Most of the ICT security counter-measures are only on an ad-hoc basis and not good enough. For example neither documentation nor back-up plans exist for both software and data.

4.2.2. Institute Z. The existing technical controls are only on an ad-hoc basis and depend on individual initiatives. For example, not all the systems are up-to-date with respect to revisions and patches. In general, following the completion of the ICT policy and master plan, the institute is in the process of implementation. This involved formation of a new ICT department which did not exist before.

4.2.3. Institute V. The institute has recently concluded the deployment of institute-wide local area network infrastructure. Small, isolated Local Area Networks, which have been operating separately, and individual PCs, are now in the institute's network. Technical control is still on an ad-hoc basis, with some effort being made towards a proper technical control.

4.3 Physical and environmental controls

4.3.1. Institute X. There are some procedures in place for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media, but they are not documented. Procedures for managing visitors also exist but are neither documented nor enforced. The same applies to workstations and other components that allow access to sensitive information. However, the study has indicated that personnel responsible for handling critical information have self initiatives for physically and logically safeguarding and preventing unauthorised access to the systems under their control.

4.3.2. Institute Z. The situation regarding physical and environmental controls is the same as institute **X**, except that the security guards are outsourced. The environment in which most of the workstations are kept is not very suitable for their proper functioning.

4.3.3. Institute V. The institute has implemented well thought physical and environmental security, having physically isolated all small networks which handle critical/sensitive information. Back-ups are stored off-site and processes for sensitive information are being discarded. Physical security (guards) is also provided and well managed.

5. Discussion: Problems and Consequences

5.1 Strategic level

The study has indicated that none of the institutes had previously a practice of actively incorporating ICT security into their strategic plans. Institute **X** did incorporate ICT security into its strategic plan, but no plans for its implementation have ever been laid down, apart from uncoordinated and ad-hoc initiatives at individual or departmental level. Institute **Z** has

recently, in year 2004, incorporated ICT security into its strategic plans, but it is not yet operational. In the third case, institute **V** is at the policy formulation stage.

By not having ICT security policy in the concerned institutes, as revealed here, they have gone against the international best practices for ICT security management. Without an overall ICT security policy in an institute, no starting point and reference framework can exist on which all other ICT security sub-policies, procedures, standards, and countermeasures must be based. Existence of such a policy would show top management commitment towards all ICT security aspects, while its absence would render all efforts towards ICT security anchor-less and hence useless. Sadly, ICT security is perceived to be the duty of the IT department or merely a technical issue.

5.2 Operational level

As can be deduced from the study findings above, the complex problem of ICT security has been relegated to the IT department or rather treated as a technical problem, with no relevant organisation-wide ICT security policy. While this does not meet the institutes' ICT security requirements entirely, taking both technical and non-technical security measures will go a long way towards achieving them. There needs to use a holistic approach to cater for the multidisciplinary nature of the ICT security problem.

There are obvious gaps at the operational level in each of the studied institutes when measured against existing standards such as ISO 17799 [6], in terms of practices and procedures. For example whatever counter-measures they had lacked documentation, configuration, change management and incident management. In addition simple measures like data back-up plans, training of end users, etc. are not taking place. Obviously these are not issues to be handled entirely by the technical or IT departments alone, as top management support and commitment is of the utmost importance [7, 8]. However, this is not the case, as reflected in the strategies and budgets apportioned for ICT security.

In addition to technical controls, there are several other non-technical ones, which are important in overall ICT security. It is not implied here that all of these others are missing because some are in place but are not coordinated in a way which enhances ICT security. For example; with the introduction of computers in all institutes, it prompted special reinforcement of the access controls in the physical locations where the systems have been deployed. While physical control may secure the hardware, it may not secure the data in them.

Cultural control might also help, as most people tend to value tangible things like PC hardware, but not the information in it. As we enter the information economy it is high time to change the culture to reflect contemporary economic trends. We normally protect what we value! It is now intangible economy.

None of the three organisations had designated ICT security personnel/unit. Instead, systems administrators, as well as their normal duties, are expected to be able to handle security issues as well, for which most of them have not been trained and they are not necessarily knowledgeable. This, in turn, results in security controls implemented, being mainly those built into products like operating systems and applications, which are not enough. In the event that a security product like a firewall or anti-virus is in place, the configurations are based on the individual's understanding and not according to the institute's ICT security policy, which is missing.

The study has revealed that the contingency and disaster recovery planning in the institutes are only on ad-hoc basis. There is no business continuity or emergency operations plan for responding to emergencies related to ICT risks.

5.3 Ethical cultural legal Level

Since ICT is relatively new for society in general in this part of the world, most people do not know the "do's and don'ts" when it comes to its use with respect to relevant ethics. Our experience in this area of ICT and its use in the country shows that although there may be some ethics governing computer and related technology use, these have not been documented here in accordance with our culture, in the form of codes of conduct for computer use and distributed to the users. Such codes of conduct can provide another dimension of control when it comes to ICT security because people will be aware of what is allowed and what is not. For example, browsing a suspicious website or downloading untrustworthy programs using a workplace computer may lead to the computer being contaminated with viruses/worms and or create backdoors for hackers to own and misuse the machine. This poses a serious threat to the organisation's ICT assets [8].

Also, at the country level, we lack the necessary ICT legal framework to assist in ICT security issues and controls. This is an area that needs immediate government intervention and action. The new (2003) national ICT policy [4], which is already in effect, has

provision for that but its implementation is what we are waiting to see.

5.4 Consequences

The likely consequences of the potential damages due to ICT risks can be summarised as follows: service interruption—due to failure of the systems involved in handling core services. This can result in the loss and/or disclosure of critical information as well as, direct loss and liabilities. Eventually these can lead to loss of reputation and credibility of an institute as a result of say, examination leakages, tampering with examination records, examination grading and certificates processing. In addition, extra costs and financial losses due to security failures in computerised financial information systems, loss of library services and other online information such as lecture materials. Further, loss of confidence by staff/students and infringement of privacy/copy rights are also possible.

6. Conclusion

The impact of the ICT diffusion and use on the studied institutes has been increased efficiency and flexibility in providing core services (education, research and community services) where such services have been computerised. However, such benefits will be short-lived if this transformation from manual to computerised methods of offering education is not given adequate planning beforehand and supported by the necessary infrastructure, both at the national and organisational levels. This should be reflected in their ICT strategies.

Currently, the necessary infrastructure is missing at the national level, i.e. laws, regulations, policies etc. for digital information security, since a national ICT security policy is non-existent. On the other hand, national (traditional) policies exist on how to handle critical information securely (like hard-copy paper files) in the physical world and these are known to all concerned and are being implemented accordingly. Now that a new way of handling information is being slowly introduced and implemented (ICT), governments in the developing countries, which aspire to acquire and use ICT, should take the initiative in transforming the traditional information security policies into relevant policies to cater for digital information security.

Thus, at an organisational level it would be mandatory to acquire, deploy and use ICT in such a way as to guarantee sustainability of the systems and security of the information as per the national ICT security policies. Referring to the findings of the study, such a national ICT security policy would put an end to the notion, as observed at the organisational level, that ICT security is the problem of IT departments, and is a technical rather than a strategic problem. It would require overall management procedures involving the entire organisation.

Consequently, organisations/institutes employing ICT would be required by law or regulatory body to have a comprehensive information security policy in place, in accordance with acceptable standards and relevant to its environment, to minimise the likely risks due to ICT usage. This would pave the way for possible integration of ICT currently being developed and deployed in the developing world with those of the developed world, thus hopefully reducing the ever-increasing digital divide through operational participation.

Limitations: According to [Jacobs et al. 1992: 45] in [5], the outcome of this kind of research may not be generalised. However, it gives a much richer and deeper understanding and description of the studied phenomena.

7. References

[1] C. Alberts and A. Dorofee, "*Managing Information Security Risk", The OCTAVE approach*, Addison Wesley, USA, 2003.

[2] C. 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.

[3] J. K. Bakari, L. Yngström, C. Magnusson and J. A. Chaula, "Towards Managing ICT security in non-commercial organisations in developing countries" *ISSA 2004*, Information Security South Africa, Johannesburg, 2004.

[4] Tanzania National ICT Policy, March, 2003. Also available at http://www.tanzania.go.tz/pdf/ictpolicy.pdf [Accessed on 02nd April, 2005]

[5] Research Method, *An Overview of some research methods* http://www.petech.ac.za/robert/resmeth.htm [accessed on 23rd November 2003].

[6] ISO 17799.

[7] B. V. Solms and R. V. Solms, "The 10 deadly sins of information security management", *Computers & Security*, Vol.23 No 5 ISSN 0167 –4048, 2004, pp. 371-376.

[8] Bishop, M, *Computer Security, Art and Science*, Addison Wesley, USA, 2003.

PAPER II

The Mitigation of ICT Risks Using EMITL Tool: An Empirical Study

Reprinted from

The Proceedings of the International Federation for Information Processing (IFIP)
Volume 193,TC-11 WG 11.1 & WG 11.5, Joint Working Conference on
Security Management, Integrity, and Internal Control in Information Systems,
eds. Dowland, P., Furnell, S., Thuraisingham, B., Wang, X. (*Springer*)
Fairfax, Virginia, Washington, USA
December 1 - 2, 2005
pp. 157-173, ISBN: 0-387-29826-6.

THE MITIGATION OF ICT RISKS USING EMITL TOOL: AN EMPIRICAL STUDY

Jabiri Kuwe Bakari[1], Christer Magnusson[2], Charles N. Tarimo[3] and Louise Yngström[4]

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: {si-jba[1], christer[2] si-cnt[3], louise[4]}@dsv.su.se

Abstract: As the dependence on ICT in running organisations' core services is increasing, so is the exposure to the associated risks due to ICT use. In order to meet organisational objectives in ICT dependent organisations, risks due to ICT insecurity need to be addressed effectively and adequately. To achieve this, organisations must have effective means for the management of ICT risks. This involves assessment of the actual exposure to ICT risks relevant to their environment and implementation of relevant countermeasures based on the assessment results. On the contrary, in most organisations, ICT security (or ICT risk management) is perceived by the top management as a technical problem. As a result, measures for ICT risk mitigation that are ultimately put in place in such organisations tend to be inadequate. Furthermore, the traditional way of managing risks by transferring them to the insurance companies is not yet working, as it is difficult to estimate the financial consequences due to ICT-related risks. There is, therefore, a need to have methods or ways which can assist in interpreting ICT risks into a financial context (senior management language) thereby creating a common understanding of ICT risks among technical people and the management within ICT-dependent organisations. With a common understanding, it would be possible to realise a coordinated approach towards ICT risk mitigation.

This paper is an attempt to investigate whether ICT risk mitigation can be enhanced using a customised software tool. A software tool for converting financial terminologies (financial risk exposure) to corresponding ICT security terminologies (countermeasures) is presented. The Estimated Maximum Information Technology Loss (EMitL) tool is investigated for its suitability as an operational tool for the above-mentioned purpose. EMitL is a tool utilised in a framework (Business Requirements on Information Technology Security - BRITS) to bridge the understanding gap between senior management and the

technical personnel (when it comes to ICT risk management). This work is based on an empirical study which involved interviews and observations conducted in five non-commercial organisations in Tanzania. The study was designed to establish the state of ICT security management practice in the studied organisations.

The results of the study are being used here to investigate the applicability of the EMitL tool to address the observed state. The results from this study show that it is possible to customise EMitL into a usefully operational tool for interpreting risk exposure due to ICT into corresponding countermeasures. These results underline the need to further improve EMitL for wider use.

Key words: ICT Risk management, EMitL tool, Countermeasures

1. INTRODUCTION

The demand for adequate ICT security in ICT-dependent organisations continues to grow as the types and patterns of threat change. ICT security forms an important component of modern business strategic planning processes as well as the operational environment. Risks due to ICT insecurity need to be addressed effectively and adequately if an ICT-dependent organisation is to meet its business objectives. ICT security risks are threats that can have an impact on the availability, confidentially and integrity of information, as well as communications and services. Thus, organisations must have effective means for management of ICT-related risks specific to their environments (Frisinger, 2001).While this can be viewed as a common business-risk problem which calls for traditional risk management methods, the existing traditional methods for handling traditional business risks in organisations (conventional notions of risks and available styles and methods such as insurance coverage) tend to be difficult to employ directly for ICT risks (risks pertaining to computerised information systems). Uncertainties in quantifying ICT- related risk, make it a special kind of risk. Often, as a consequence, ICT-related risks are either left out in the overall risk-assessment process or addressed by ad-hoc technical controls, which make it hard to ensure whether the pertaining risks have indeed been adequately hedged to meet the business objectives. To avoid duplication of effort, it is appropriate and desirable to combine information security risk assessments with other business-related risk assessments.

ICT security should be a component of the overall risk management process within an organisation. ICT security is risk management with a focus on ICT (Blakley, B., McDermott, E., and Geer, D., 2001). Risk management is part of management's responsibility. However, there is often a tendency by the management to neglect or omit ICT security problems from the general organisational risk management process. This is due to inadequate understanding of ICT security issues and (as noted earlier) difficulties in having reliable estimations of the financial consequences caused by ICT security problems. Hence, application of traditional ways for managing risks by having them transferred to the insurance companies is not straightforward. Further, ICT security is perceived by top management to be a technical problem. There is, therefore, a need to have tools which can assist in interpreting ICT risks into a financial context (senior management language) and thereby creating a common understanding of ICT risks among technical people and the management within ICT-dependent organisations. With a common understanding, it would be possible to attain a coordinated approach towards ICT risk mitigation.

Approaches such as OCTAVE, COBIT, ITIL, ISO 17799 etc., (ISACA, 2005; ITIL, 2005; ISO 17799) have been developed to address the problem. Each of these addresses the problem from a specific perspective, based on certain philosophical assumptions. All of these various forms of approaches are aimed at providing the means for ICT risk management.

ICT risk management in an organisation begins with identification of what needs protection and why. It also involves being able to have a notion of the extent of the pertaining risks either qualitatively, quantitatively or both. After risk assessment, the organisation must take appropriate steps to mitigate the identified risks. Specific items in such identified risk elements could be aspects such as: ICT security, Physical security risks, Deficiencies in personnel knowledge, training and practices, Security documentation practices, etc. It is not our intention to review or analyse existing ICT risk management approaches in any detail, as that has been addressed in various literature such as in (Frisinger, 2001, Magnusson, 1999, Baskerville, 1993, Anderson, A., et al, 1991, Alberts & Dorofee, 2003). Instead, the intention here is to investigate whether ICT risk mitigation can be enhanced using a customised software tool. Thus, a software tool for converting financial terminologies (financial risk exposure) to corresponding ICT security terminologies (countermeasures) is presented and evaluated. The Estimated Maximum Information Technology Loss (EMitL) tool is investigated for its suitability as an operational tool for the above-mentioned purpose. EMitL is a tool utilised in the Business Requirements on Information Technology Security (BRITS) framework to bridge the understanding and perception gap between the senior management and the technical expertise as regards to

ICT risk management. The tool was developed for and tested in commercial organisations. An attempt is made here to utilise the tool in non-commercial organisations.

2. METHODOLOGY

This study employs data from a previous study which had to do with investigation of the state of ICT security management as being practised in five non-commercial organisations (X, Y, Z, U and V) (Bakari, 2005; Bakari et al., 2005). Hence, the results from the study are used here as input to investigate the applicability of the EMitL tool in addressing the observed state. By putting the collected data into the tool, the tool generates a set of corresponding countermeasures that would have been in place given the observed state. The generated countermeasures for each organisation are then analysed to see their relevance to the observed state. Figure 1, below shows a pictorial representation of the process.

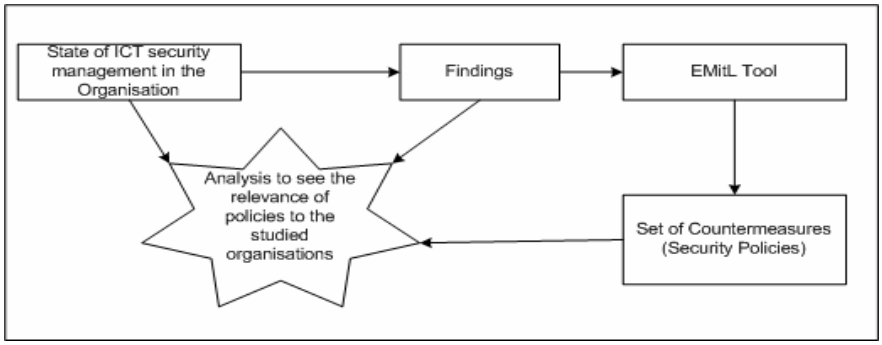


Figure 1. Summarising input and output to EmitL tool

In the next section we briefly describe the EMitL tool.

3. EMITL TOOL

EMitL is an interactive database-based tool designed to generate security countermeasures based on an organisation's exposure to ICT-related risks. EMitL is utilised as a component of the BRITS framework, which is a Systemic-Holistic framework, combining finance, risk transfer, ICT and security in a coherent system. The framework can be viewed as consisting of

the top management and the technical personnel regimes with EMitL acting as a bridge between them, as shown in figure 2 below. The resulting conceptual structure is known as the BRITS framework. BRITS was developed to address the communication discontinuity existing due to the lack of common terminologies between the organisation's top management (potential risk exposure—financial) and technical people (ICT security experts—technical). Thus in the framework, the EMitL tool converts financial terminology into ICT security terminology and vice versa.

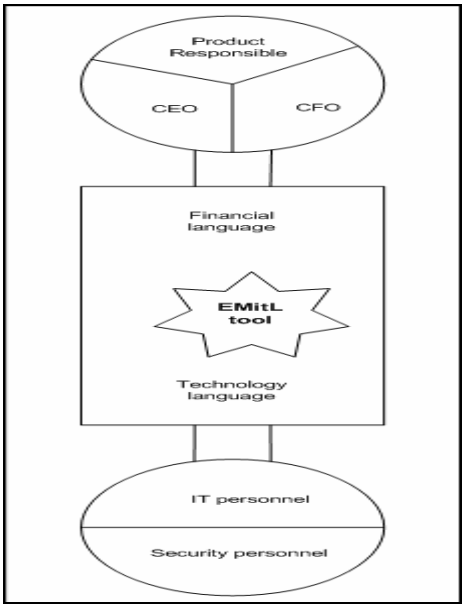


Figure 2. Function of EmitL tool: Source (Magnusson, 1999)

By bridging the two components, the vulnerabilities in ICT can be explained in financial terms, as well as in technical terms. The tool is conceptually structured into three groups; logical, physical, and organisational. It consists of approximately 1,000 security requirements in total. These include: authentication mechanisms; protection of accountability or non-repudiation; access control measures; protection of routing patterns; prevention against denial of service attacks; measures against data and program modification, insertion or destruction. Physical security countermeasures include: power supply and spare parts, fire protection, prevention of water damages, access and mechanical protection. Organisational security countermeasures include: roles and responsibilities, installation, configuration and operation of software and hardware and protection of intellectual property. In addressing these measures, the tool has

considered four levels of security which comprise the following ICT areas: user workstation, a server, network applications, local area networks, remote connections and common ICT. Common ICT areas include organisational issues such as, user identities and user management, general access control and accountability principles (Magnusson, 1999, P. 165-168).

EMitL maps potential damage exposure against security properties and then generates the corresponding countermeasures. The countermeasures are grouped into four security levels, starting with security level 1 (low security) to level 4 (highest security). Figure 3 below shows the snapshot of the EMitL tool interface. In the figure, for example, the hedge policies 'Liability' for 'service interruption', 'Defamation', 'Infringement of Privacy' and Infringement of trademark' were the input.

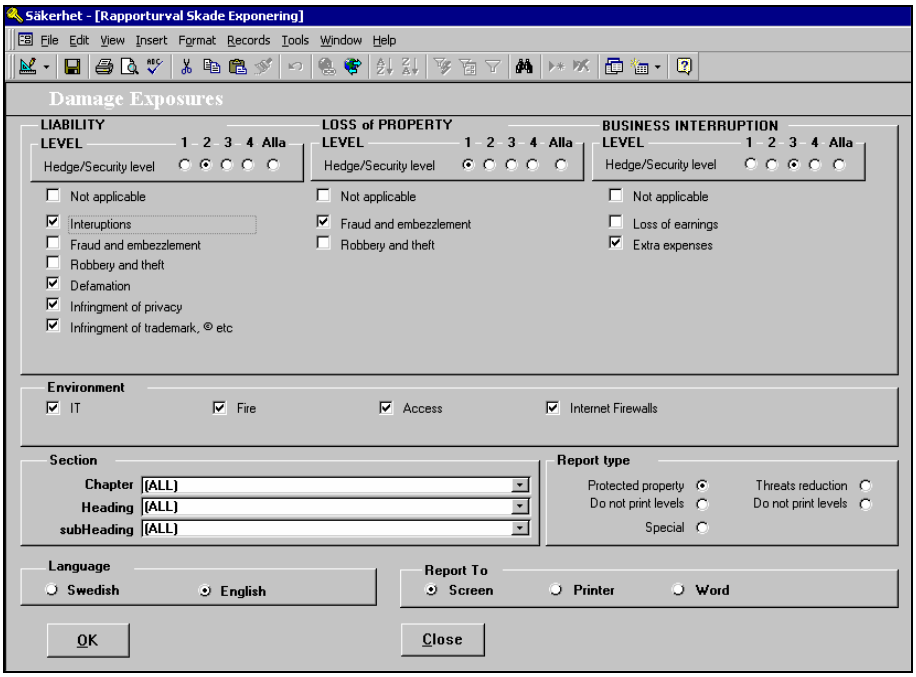


Figure 3. Snapshot of the EmitL tool interface

The level of protection required in this particular example is equivalent to hedge level 2. Consequently, the output are countermeasures against ('service interruption', 'defamation', 'infringement of privacy' and 'infringement of trademark') based on the adequate countermeasures at security level 2. In the framework, the damage exposure is divided into Liability, Loss of property and Service interruption.

Table 1 maps damage exposure against affected ICT security properties. The outcome of running the interactive database with the obtained parameters from an organisation is a set of countermeasures which should have been in place given the input parameters provided in the tool. This set of countermeasures is produced as a report.

Table 1. Damage exposure and ICT security properties

	ICT security Properties		
Damage exposure	Integrity	Availability	Confidentiality
Liability			
Service Interruption		**X**	
Fraud & Embezzlement	**X**		
Robbery & Theft			**X**
Defamation	**X**		
Infringement of Privacy			**X**
Infringement of Trademark, © etc.	**X**		
Loss of Property			
Fraud & Embezzlement	**X**		
Robbery & Theft			**X**
Service Interruption		**X**	

Source: (Magnusson, 1999, P. 143)

The report is compared with the current organisation's ICT practices in order to estimate the security awareness and control in the organisation. This could further assist in sorting out among the generated countermeasures which ones are being practised by the organisation and which are not. The result of comparisons is a state of security documented in the form of a survey report that gives an overview of the security awareness and vulnerabilities in the organisation. This report can further be used to estimate the Expected Maximum Loss (EML) if the identified risks are not mitigated.

4. BRIEF STATE OF ICT SECURITY IN THE STUDIED ORGANISATIONS

Following the earlier study on the subject (Bakari, 2005), the following are (in brief) the findings. The dependency on ICT to run core services has been observed to be substantial and is continually growing in the studied organisations. Analysis of relevant ICT security issues pertaining to the studied environment yielded different results at different levels. For

example, at the strategic level there is no defined budget for ICT security, while at the operational level, the complex problem of ICT security is perceived to belong to the IT departments or rather treated as a technical problem. Organisation-wide ICT security policy is non-existent in the studied organisations. Table 2 indicates the state of ICT security as regards to budgets apportioned to ICT and the presence of ICT security policy.

Table 2. ICT Security budget and status of ICT security Policy

ORGANISATION	ICT BUDGET	ICT Security Budget	ICT Security Policy
X	3.2%	No	Non-existing
Y	5%	No	Outdated /Directed to IT staff, but not aware of its existence
Z	0.5%	No	Non-existing
U	1.6%	No	Non-existing
V	2%	No	In preparation

In the study, to establish the status of countermeasures in place, a separate interview with IT managers and system administrators was conducted. A typical example of the questions was “Are there any documented policies and procedures for physical access control of hardware and software?” The results of responses on whether or not the countermeasures are being practised show that most of the countermeasures are not practised as indicated in figure 4. The few practised countermeasures are mostly on an ad-hoc basis. The interpretation of the results was according to (Alberts and Dorofee, 2003) wherefrom the questionnaires were originally adopted. For example, looking at the issues related to contingency and disaster recovery, none of the organisations was found to be practising. The responses for the state of basic ICT security issues and practices indicate the existence of uncoordinated low level ICT security activities and these are mainly based on individual initiatives within departments. Service interruption has been observed to be a major potential problem, which could result in unavailability of the services and consequently cause extra expenses. Finally, we would like to highlight here that, while the state of ICT security is not good enough, the perceived low insecurity incidences reported should not mean that there are no potential threats. Actually, the observed situation poses the greatest threat! Simply put it means that there is a big problem in place but its existence and magnitude is not known.

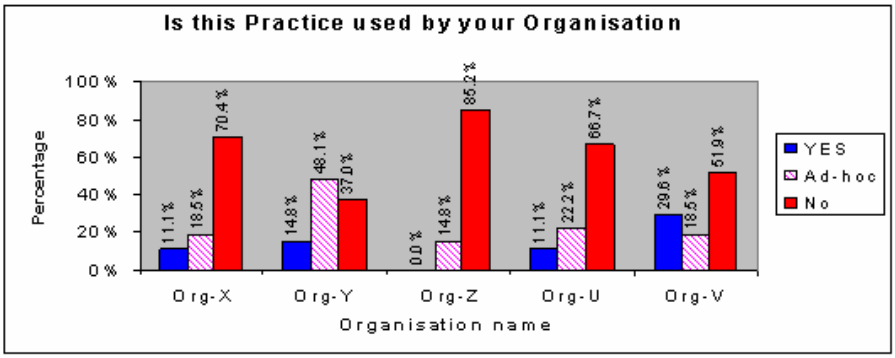


Figure 4. Responses on the countermeasures being practised by organisation

Note:

YES - If the practice is always or nearly always used. In the situation where there were many respondents, 75% or more respondents was considered YES.

Ad-hoc - If the practice does exist but not used very much, not documented and not communicated to staff, or used by some departments or individuals only

No - If the practice is not used or not used very much. In the situation where there were many respondents, 75% or more respondents was considered as No.

5. FINDINGS AND DISCUSSION

5.1 Results of subjecting the findings from the organisations to the EMitL tool

Using data gathered in responses from the top management and operational management, analysis of the same was performed for each organisation. The results are summarised in table 3. 4 represents the highest level of potential risk, 3 indicates medium—high, 2 indicates medium, 1 indicates low and 0 (zero) means not applicable. The EMitL tool interface has only one hedge policy level/security level for each set of damage exposures. Therefore an assumption had to be made where more than one security level is indicated, in order to increase the overall security level. This means one has to consider a higher security level where more than one security level exists. Results from each column were summarised first and then fed into the EMitL tool (See figure 3 in section 3 above). Table 4 shows how the security levels (columns –ARL) had been assumed to reflect the level that appears with the highest frequency.

Table 3. Damage exposure levels (Security levels)

Damage exposures	Damage exposure levels (Security level)				
	Organ. X	Organ. Y	Organ. Z	Organ. U	Organ. V
Liability					
Service Interruption	1	0	0	4	0
Fraud & Embezzlement	0	2	0	2	0
Robbery & Theft	0	0	4	2	0
Defamation	3	2	3	1	2
Infringement of Privacy	2	2	2	2	2
Infringement of trademark,© etc.	2	0	3	0	2
Loss of Property					
Fraud & Embezzlement	1	4	4	3	1
Robbery & Theft	0	0	2	2	0
Service Interruption					
Loss of sales	0	0	0	4	0
Extra expense	3	4	3	4	3

In case the same frequency is observed, a higher security level is assumed in order to increase the level of assurance. In the table organisation **X** had ARL 2, 1 and 3 respectively as shown also in the interface in figure 3 (section 3 of this paper).

Table 4. Showing different input parameters to database EmitL

Organisation	Liability						A.R.L	L/Property		A.R.L	B/Interrp		A.R.L	Output
	BI	FE	RT	DE	IP	IT		FE	RT		LS	EE		Countermeasures
X	√	×	×	√	√	√	2	√	×	1	×	√	3	847
Y	×	√	×	√	√	×	2	√	×	4	×	√	4	802
Z	×	√	√	√	√	√	3	√	√	3	×	√	3	880
U	√	√	√	√	√	×	2	√	√	3	√	√	4	803
V	×	×	×	√	√	√	2	√	×	1	×	√	3	847

Key:

BI – Business Interruption
FE - Fraud and Embezzlement
RT – Robbery and Theft
DE – Defamation
IP – Infringement of Privacy
IT – Infringement of Trademark
A.R.L – Assumed Running Level (EMitL – database)
× - Not applicable
√ - Applicable

The outcome generated after running the EMitL tool with the supplied parameters from table 4 is a report consisting of various security countermeasures. The report can be viewed on screen or exported to a Word file and printed. Depending on the parameters supplied for a particular organisation, the length of the generated reports typically ranged from 90 to 108 pages with countermeasures ranging from 802-880 (see last column – table 4). The output countermeasures consist of logical security measures structured into four security levels (security level 1, 2, 3, and 4). These

measures are mapped to IT security properties, confidentiality (C), Availability (A) and Integrity (I). Some measures protect only one security property (referred to as unique measures), some protect two security properties (referred to as dual measures) and some protect all three security properties (referred to as generic measures).

An analysis was then made to find out to what extent a given type of security countermeasure addresses the security property and at what security level. In the next section we present the results of the analysis.

5.1.1 Unique measures

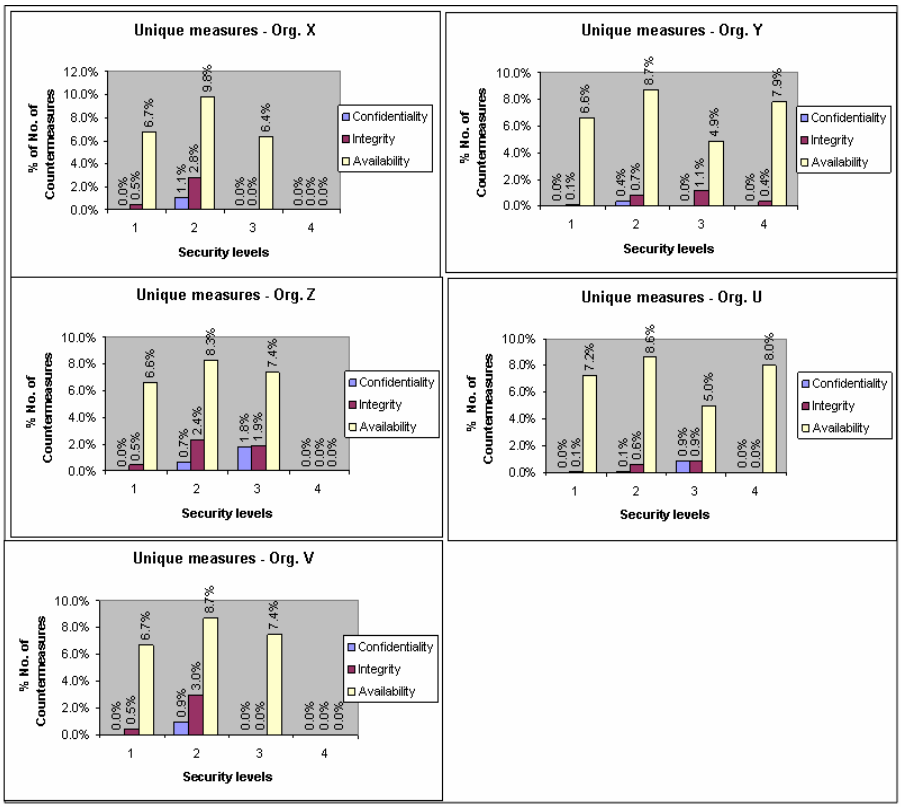


Figure 5. Percentage No. of Unique countermeasures vs. Security levels- Org. (X,Y, Z, U, V)

The focus of unique measures from the reports produced was found to be mainly on availability measures. Figure 5 presents the % number of unique measures plotted against security levels. By looking at the outcome of unique measures in all five organisations, we can observe that the focus was mainly on availability measures.

The analysis indicates that most of the countermeasures address fire evacuation route, storage, fire plan, how to handle fire-fighting equipment, automatic extinguisher systems, training and drills. The availability measure is used to benchmark ICT systems belonging to products that are exposed to service interruption and liability claims due to service interruption. An example of unique measure output from the database EMitL is given in example box 1.

Example box 1

Information

Security Level 1

2040 The target group for all fire prevention information shall be all personnel.

Property protected:Availability

5.1.2 Dual measures

Dual measures address two security properties. The dual countermeasures (Availability and Confidentiality) which carry more than 30% of the measures were found to be about "Mechanical access control" where most of the proposed measures could be at a very advance level as compared with the status of the organisations studied. Figure 6 presents the percentage number of dual countermeasures vs security levels. Example box 2 shows a sample of dual countermeasures.

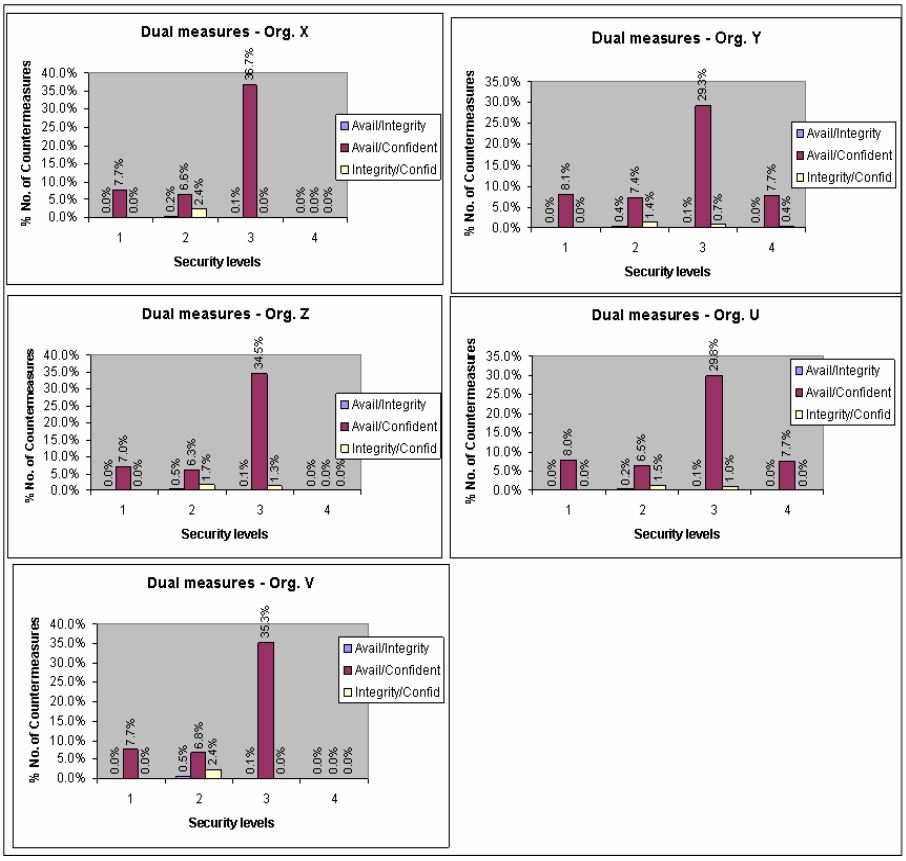


Figure 6. Percentage No. of Dual countermeasures vs security levels – Org. (X, Y, U, V, Z)

Example box 2:

Motorised pedestrian gates

Security Level 1

1810 All equipment, products and/or constructions for lock and armature units shall be of suitable design for their function, in good working order and be installed in the correct fashion.

Property protected:Confidentiality, Availability

Security Level 2

1820 If the gate is equipped with a pull handle, the locking mechanism shall consist of a single latchbolt lock with interlocking striking plate. If a trigger handle is installed, locking shall be carried out with a double latchbolt lock with an interlocking striking plate. A retaining mechanism in the form of a lock cylinder ring shall be installed on both inner and outer sides of the door. Electric striking plates shall be of extra strength construction. The automatic swing door function shall be conditioned on the status of the electric striking plate (locked/unlocked).

Property protected:Confidentiality, Availability

5.1.3 Generic measures

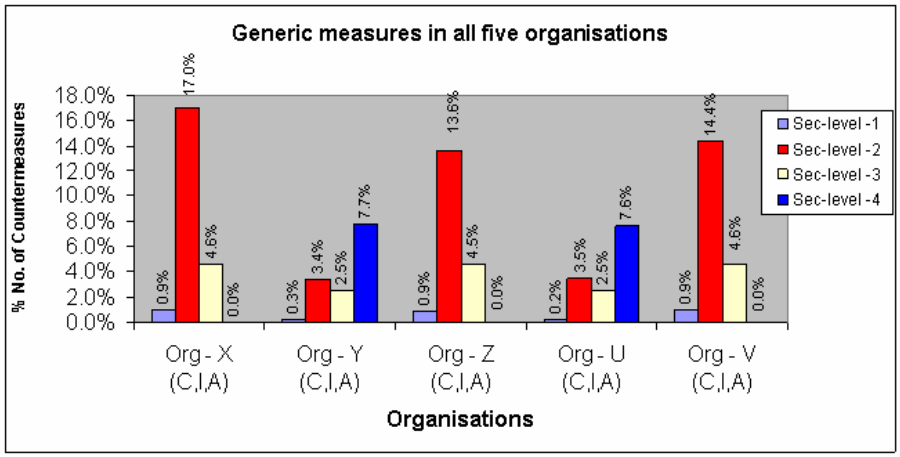


Figure 7. Percentage No. of Countermeasures vs. security levels – Org. (X, Y, Z, U, V)

Generic measures address all three security properties (figure 7). 13.6%, 14.4% and 17% of the total countermeasures for organisations X, Z and V respectively are at level two which was found mainly to addresses organisational and procedural measures. These included roles and responsibilities (See example box 3).

Example box 3:

Organisation and Procedures

Roles and Responsibilities

Security Level 2

1520 Security incidents or violations observed by system administrators, operators, or any user shall be reported to the security officer in charge.

Property protected:Confidentiality, Integrity, Availability

The requirement (see example box 3) could be seen as a measure to primarily protect confidentiality. However, this measure also protects (though indirectly) integrity and availability. For example, if an intruder manages to get the system administrator's password (which means violating confidentiality) and use it to gain access to core systems, it means the intruder can gain access to critical systems and thereby perform unauthorised modification of the systems or data (in this case violating integrity). Finally the intruder can cause operational breakdown (system malfunction) and thereby (violating availability) (Magnusson, 1999).

5.2 Discussion

An analysis of the state of ICT security in the studied organisations indicates that no ICT security policy existed in any of the organisations and the few existing technical procedures were on an ad-hoc basis. The results from the EMitL tool in the form of countermeasures that should have been in place seem to address most of the identified gaps at the operational and technical level when the implementation is customised to the environment. For example, in the dual countermeasure, the generated countermeasure from the tool about mechanical access control was suggesting automatic gates which are on the advanced side with respect to the current situation of the studied environment. Hence, customisation of the tool in that respect could lead to the relevant results. With reference to figures 5, 6 and 7 above, we could see that the countermeasures addressing security property "Availability" feature with a high frequency of occurrence for unique measures and the same is true when we look at dual measures "Availability and confidentiality" countermeasures which also have a high frequency of occurrence (from 29.3% to 36.7%). This security property is against the damage exposure "Service interruption" (See table 1 in section 3 above) and appears to be the major concern in the studied organisations by causing more extra expenses.

The study has indicated that the tool could enhance ICT risk mitigation in some ways. As noted earlier, there was a communication gap between the top management and the technical personnel with respect to ICT risks and their controls. The top management is expected to understand that ICT security is a business problem rather than a technical one and on the other hand the technical people need to understand that ICT security is more than a technical problem (it is more than firewalls, IDS and antivirus!). Using the tool, it was possible to bridge the understanding gap due to differences in perspectives and the language used between the top management and the technical people in an organisation. Using risk information from the top management, the tool generates relevant countermeasures for the environment which would need customisation. However this depends very much on accuracy in getting the organisation's actual risk exposure at the stage of establishing potential risk exposure pertaining to that particular organisation. Also, at a higher level, the tool helps in giving a rough direction of what needs to be done in order to manage ICT-related risks. This comes out in the form of a Survey Report as described in this paper. According to the previous analysis and discussion above, there is relevance between the observed ICT security state and the proposed countermeasure from the tool, although some of the suggested countermeasures need

customisation to match the actual environment. This proves its usefulness and suitability for the purpose.

The downside of the tool is as follows. It needs customisation for each organisation as different organisations have different security requirements and hence it is not something that can be used directly. The database engine that contains the countermeasures needs to be updated continuously to reflect the changes in ICT risks profiles. Thus, it suffers the same limitations as the ones suffered by anti-virus tools.

When comparing EMitL/BRITS with other ICT security methods such as ISO 17799, OCTAVE, ITIL, COBIT etc., we came to the conclusion that each of these other methods addresses a portion of the overall ICT risk management problem while EMitL provides a means of combining them all together. For example, OCTAVE serves as the first step when approaching ICT risk management problems; COBIT is used mainly for auditing; ISO 17799 is mainly used to address HOW issues, etc. On the other hand, the idea behind BRITS-EMitL is to make it possible to provide a framework that makes use of all of these in a coherent system to address the organisation's ICT risk management problem.

6. CONCLUSION

This paper has attempted to investigate the applicability of the EMitL tool in mitigating ICT risks using the empirical data collected from five non-commercial organisations in Tanzania. The information captured from the top management in their language (financial), which was later entered into the tool, resulted in countermeasures which would have been in place in the respective organisations. On analysis, the generated countermeasures were seen to mitigate potential risk exposures which were pointed out by the management as discussed in the paper. This implies that the EMitL tool could be a useful tool in bridging the identified communication gap between the management and technical departments when it comes to managing ICT-related risks.

However, the usefulness of the tool needs to be kept current with respect to the changes in ICT security threats, organisation needs, and technologies. Ongoing improvements to the database (security measures, practices, and technology) are necessary to keep up to date with potential attackers and to keep abreast of the organisation's service needs.

REFERENCES

Alberts, C., and Dorofee, A., 2003, "Managing Information Security Risks", the OCTAVE Approach, Addison Wesley, USA.

Anderson, A., and Shain, S., 1991, "Risk management in Information Security hand book, Macmillan publishers Ltd.

Bakari, J. K., 2005, "Towards A Holistic Approach for Managing ICT Security in Developing Countries: A Case Study Of Tanzania", Ph.L thesis, Department of Computer and Systems Science, SU-KTH, Stockholm.

Bakari, J., Yngström, L., Magnusson, C., and Tarimo, C. N., 2005, "State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case study", The 5th IEEE (ICALT 2005), Kaohsiung, Taiwan. Pp. 1007-1011

Baskerville, R., 1993, "Information Systems Security Design Methods: Implication for Information System Development", ACM Computing Surveys, Vol.25, No.4.

Blakley, B., McDermott, E., and Geer, D., 2001 "Information Security is Information Risk Management" ACM Press, New York, USA.

Frisinger, A., 2001, 'A Generic Security Evaluation Method for Open Distributed Systems' Ph.D Thesis, Department of Teleinformatics, Royal Institute of Technology, Sweden.

ISACA, 2005, (April 15, 2005) http://www.isaca.org

ISO 17799, Information technology – Code of practice for information security management

ITIL, 2005, (April 15, 2005); http://www.itil.org.uk/

Magnusson, C., 1999 "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.

PAPER III

Outsourcing ICT security to MSSP: Issues and Challenges for the developing world

Reprinted from

The Proceedings of Information Security South Africa (ISSA),
from insight to foresight Conference,
eds. Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM,
Sandton, Johannesburg, South Africa
July 05-07, 2006
ISBN: 1-86854-636-5

OUTSOURCING ICT SECURITY TO MSSP: ISSUES AND CHALLENGES FOR THE DEVELOPING WORLD

Jabiri Kuwe Bakari[1], Christer Magnusson[2], Charles N. Tarimo[3] and Louise Yngström[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], cmagnus[2], si-cnt[3], louise[4]}@dsv.su.se

ABSTRACT

The overall use and development of ICT in developing countries has been faced with a wide range of constraints and challenges. These constraints may concern culture, infrastructure and education, and involve social, legal, political or economic issues. Numerous problems related to each of these issues have been observed. The problems may include, for example the absence of ICT policies, implementation procedures, a general lack of appropriate knowledge of ICT (among suppliers, managers, planners and users), too few trained /skilled ICT personnel or simply budget constraints. Among the critical issues that call for immediate attention and action are the security of information assets and processing systems. ICT security management poses a big challenge given the range of constraints mentioned and is critical for the trust and normal functioning of the various ICTs deployed.

As is widely known, ICT security management process needs a holistic approach with experienced personnel, right policy and procedures, and the right technology. It also requires continuous monitoring and continuous threat intelligence in order to achieve and maintain sufficient security in an organisation. It follows then that achieving adequate ICT security management is a big challenge especially for organisations whose core services is not ICT. The idea behind outsourcing ICT security is based on the assumption that engaging a managed ICT security provider may be of great importance to such organisations, in that, like insurance, they will be relieved of their ICT security burden by transferring it to a third party. Given these presumptions many organisations worldwide may consider outsourcing their security services as a way forward in managing ICT security. However, the decision to outsource is never straightforward and is influenced by various constraints as mentioned above.

Based on some empirical data, this paper describes typical characteristics of a developing country's ICT environment from an ICT security management point of view and then discusses the suitability of the environment to benefit from outsourcing managed ICT security services. Use is made of the general merits of ICT security outsourcing as described in the numerous literature to discuss specific issues and challenges in this process that are believed to be necessary if the ICT security services outsourcing paradigm is to be adopted in developing countries with similar characteristics as those described in this paper.

KEY WORDS

ICT Security management, Managed security services, Developing countries, ICT Security outsourcing

OUTSOURCING ICT SECURITY TO MSSP: ISSUES AND CHALLENGES FOR THE DEVELOPING WORLD

1 INTRODUCTION

One of the possible alternatives an organisation can use to successfully manage its information and communication technology (ICT) security is to outsource its security services. This means transferring part or all of the risks to another organisation called a Managed Security Service Provider (MSSP). This is the same as managing ICT related risks by transferring them to another organisation—the MSSP. Managed security services (MSS) is a service used to identify and handle organisations' real-time ICT security risks by using a proven continuous management process (IBM, 2004). Services offered by MSSPs may include; assessment of vulnerabilities, detection of attacks, protection of the ICT infrastructure and reporting suspicious activities and events; incident management, including emergency response and forensic analysis; penetration testing, anti-virus and content filtering; information risk assessments, data archiving and restoration, and on-site consulting services. An example of such services is network boundary protection which includes managed services for firewalls, intrusion detection systems (IDSs), and virtual private networks (Allen et al., 2003; Sadowsky et al., 2003). In practice the service/s offered will depend on what was requested and or bargained in the contract, it is not necessary that all these services are included.

Such services whether outsourced or provided in-house are critical for the reliable security state of organisation whose core services are directly linked to the state of its information systems. However, while outsourcing is one of the solutions that are recently emerging, a careful analysis of its advantages and disadvantages should be considered before attempting to make any decision. It is true that, given the nature of ICT security problem (multi-dimension one), organisations need to have in place the right technology, experienced people, continuous monitoring, and continuous threat intelligence, in order to implement and maintain sufficient security in an organisation. Depending on the size of the organisation and its dependency on ICT, it may be difficult to cope with the huge quantity of information about security threats, which includes among other things monitoring thousands of logs from a number of devices, and responding quickly to security events. This is a challenge particularly for organisations whose core business/services is not ICT or security itself and this is where the idea of outsourcing is coming from (Magnusson, 1999; Allen et al., 2003). There is therefore a need to clearly explore the benefits and consequences of outsourcing before one makes a decision on whether or not to outsource ICT security services.

This work is based on an empirical study conducted in Tanzania between summer 2004 and February 2005. A questionnaire and face to face interview approach was used to gather and study the existing ICT security management practices in a few selected organisations. Five organisations were involved in the study with the intention of examining the state of ICT security management problems and possible potential solutions.

In this paper, an analysis of how practical it is, given the status of ICT security, for the organisations under discussion to outsource security services as a viable option is presented. The same is done for the potential managed security service providers to offer their services. The results of the study indicate that most of the pre-requisites for an organisation to outsource its security services on the one hand leave a number of questions unanswered, while, on the other hand, give the potential managed security services providers a host of hurdles to surmount if they are to be successful in offering such services in the studied environment. Hence an attempt is made here to underline issues of interest for outsourcing to be successful in such environment.

The paper is organised into the following 8 sections: section 1 introduction and background of the problem, section 2 – methodology and section 3 gives an overview of ICT security management in the studied organisations. Section 4 outlines benefits and drawbacks of outsourcing ICT security services to MSSP. Section 5 discusses issues and challenges when outsourcing ICT security services in the developing world. Discussion and conclusion are presented in section 6 and 7 respectively and finally references in section 8.

2 METHODOLOGY

This study employs data from a previous study investigating the state of ICT security management as practised in five organisations (X, Y, Z, U and V) between 2003 and 2005 (Bakari, J. K., 2005a; Bakari, J. K. et al., 2005b; Bakari, J. K. et al., 2005c). Face-to-face interview was used to gather the information where about 88.3% (68 out of 77) of the potential sampled respondents identified from the organisation structures were successful interviewed as indicated in Table 1-1.

Table 1-1: Respondents distribution

Organisation	**X**	**Y**	**Z**	**U**	**V**
Top management	1(8)	1	1	1	1
Financial Officers (CFOs)	1(1)	1	1	1*	1
Operational Management	5(20)	3	5	5	2
Operational manag. in IT Dept	9(14)	8	2	2	1
General and Technical staff	3(13)	5	3	2	3
Total	**19 (56)**	**18**	**12**	**11**	**8**

Note: The numbers in the brackets in first column represent pilot study which took place first in organisation **X.**

The selection of the respondents was based on the organisational structure and allocation of core services in a particular organisation. The questionnaires were mainly based on Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method and Business Requirements on Information Technology Security (BRITS) framework. OCTAVE was developed at the CERT Coordination Centre (CERT/CC), Carnegie Mellon University. OCTAVE is a risk-based strategic assessment and planning technique for ICT security. OCTAVE serves as an important first step in approaching information security risk management (Alberts, C. & Dorofee, A. 2003). BRITS is a Systemic-Holistic framework, combining finance, risk transfer, IT and security in a coherent system (Magnusson, C., 1999). In addition, much time was spent in the five organisations to make participatory observations and where necessary verify the collected information by going through various referenced documents (Documents referenced by the respondents during the interview). We use core services in our work to refer to the main services that the organisation is responsible for or entitled to offer and consequently achieve the objective of its existence.

Hence the results from the study are used here as foundation to discuss the feasibility of outsourcing ICT security services, at the provider's as well as the customer's end with respect to the environment studied.

3 AN OVERVIEW OF ICT SECURITY MANAGEMENT IN THE STUDIED ORGANISATIONS

As detailed in (Bakari, J. K., 2005a; Bakari, J. K. et al., 2005b, Bakari, J. K. et al., 2005c) the study involved investigation of the state of ICT security management as practised in five organisations (X, Y, Z, U and V) 2003-2005. In this section an overview of ICT security management in the five organisations studied is briefly presented.

Analysis of relevant ICT security issues pertaining to the studied environment yielded different results at different levels. For example, at the strategic level there is no defined budget for ICT security. The budget apportioned to ICT is mainly for salaries, Internet connectivity (which is relatively expensive in the studied environment) and buying ICT equipment, in particular computers. No budget was allocated to ICT security in any of the organisations included in the study. At the operational level, the complex problem of ICT security is perceived to belong to the Information Technology (IT) departments or rather treated as a technical problem. Organisation-wide ICT security policy is non-existent in the studied organisations coupled with small number of ICT staff with little or no ICT security training.

In order to establish the status of countermeasures in place, separate interviews with IT managers and system administrators were conducted. The results of responses on whether or not the countermeasures are being practised show that they are mostly on an ad-hoc basis. The responses on the state of basic ICT security issues and practices indicate the existence of uncoordinated low level ICT security activities, mainly based on individual initiatives within departments.

None of the five organisations had designated ICT security personnel/unit. Instead, systems administrators, as part of their normal duties, are expected to be able to handle security issues, for which most of them have not been trained and about which they are not necessarily knowledgeable. This, in turn, results in the security controls implemented being mainly built into products like operating systems and applications, which per se are not enough. In the event that a security product like a firewall or anti-virus software is in place, the configurations are based on the individual's understanding and not according to the organisation's ICT security policy which does not exist. ICT is still vendor driven in the studied environment and there is much reliance on vendors and consultants for knowledge and expertise. The big challenge was the observations that most individuals do not understand the magnitude of the ICT security problems and those who have an idea of the problem do not know where to start. There are some indications that ICT security is understood as ending with firewalls, anti-viruses, and physical security in the entry and exit places including where computers are accommodated. However in the absence of ICT security policies and procedures even implementations of some few countermeasures are on ad-hock basis. In addition it was also found that most people do not know the "do's and don'ts" when it comes to ICT use with respect to relevant ethics.

4 BENEFITS AND DRAWBACKS OF OUTSOURCING ICT SECURITY SERVICES TO MSSP

Before beginning the discussion on the issues and challenges involved in outsourcing ICT security services in the studied environment, it is important to briefly highlight some reasons why an organisation should or should not outsource security services by engaging an MSSP based on discussions by (Allen et al., 2003; Sadowsky et al., 2003).

Outsourcing is considered as one of the cost effective ways of dealing with ICT security management. For example the fact that ICT security threats, organisational needs, and the technology itself change very fast, necessitates organisations' ICT departments/units to recruit, train, adequately compensate, and retain skilled staff. This is an expensive endeavour. For an

MSSP, this is their main business; they are in most cases equipped with state-of-the-art infrastructure and special security operation centres.

There are equally some drawbacks of outsourcing if not done appropriately. For example a sense of ownership is very important in risk management, in particular when transferring risks to a third party. It is generally suggested that an organisation retains ownership and responsibility for secure operations and the protection of its valuable asset—information. However, in practice, many organisations may tend to ignore this, thinking that they have already transferred the 'risks' to the third party MSSP just like traditional insurances.

Another drawback is that of trust. Managing information security involves handling the valuable asset—the information of the organisation. This means that the MSSP has access to this sensitive asset, including full details about the organisation's state of ICT security and vulnerabilities. Any attempt to release such information to a third party could cause severe damage to the organisation, its reputation and credibility. Furthermore, disputes may arise during the contract period or during unexpected/unplanned termination of a contract with an MSSP. In such cases, the establishment of facts or evidences to a court of law requires special skills. Sometimes outsourcing MSS does have legal implications such as jurisdiction differences in applicable laws and regulations and the law's compatibility between the client and provider. In the absence of a legal framework, low level of knowledge on ICT related crimes among the organisations' lawyers, handling such cases becomes very complicated and expensive undertaking.

It is not our intention to discuss in detail advantages and disadvantages of outsourcing Managed ICT security in this paper, only to give an overview. The details of such discussion can be found in (Allen et al., 2003; Sadowsky et al., 2003) and other literatures.

5 OUTSOURCING MANAGED ICT SECURITY SERVICES IN THE DEVELOPING WORLD, ISSUES AND CHALLENGES

In this section issues and challenges of outsourcing Managed ICT security services in an instance of the developing world environment (the studied organisations), are briefly discussed.

5.1 Skills

Referring to the discussion on skills above, it might appear that, given the state of ICT security management, the best approach is to outsource the ICT security services. However, necessary ICT security skills are required even before undertaking the process of engaging an MSSP, to guide the management through the process of risk analysis and explore the benefit (cost/benefit analysis) of outsourcing. At times this exploration of benefits is not possible to be done by the client organisation due to lack of knowledge and hence they tend to rely entirely on consultancy. It means then they have to seek consultancy form elsewhere or trust the one that is provided by the prospective provider. In addition, in-house expertise would also be required during the implementation period, to ensure that the MSSP delivers as agreed and, later, to handle the termination of the relationship when it happens. This is a challenge in particular for organisation with similar state and operating in the environment as the ones described in the paper.

5.2 Facilities

In most cases the services offered by MSSP are conducted remotely. This requires all hardware and software to be monitored to meet certain standards of configuration and compatibility, such as uniformity in operating systems. None out of the five organisations had recommended and up-to-date facilities to handle security incidents. In some cases even proper equipment to handle day to day operations were missing. In addition, none of the organisations used standards for ICT equipment and software; as a result, different types of equipment were running on different operating systems ranging from, various versions of Windows, Linux or Macintosh, etc. Poorly

designed local area networks, power fluctuations and frequent power cuts complicate the problem further.

5.3 Implementation

Starting to implement an MSS relationship may require a complex transition of people, processes, hardware, software, and other assets from the client to the provider or from one provider to another, all of which may introduce new risks (Allen et al, 2003). This may be even more challenging when taking place in the studied organisations where none had the designated ICT security personnel/unit, ICT security policies and procedures were missing or outdated and no budget was allocated to ICT security. In addition services offered by MSSPs are mainly technical, which means that only part of the actual security problem is addressed (Ding, W. et al, 2005). Figure 1 presents a holistic view of security where the technical services as offered by an MSSP would only be parts of the solution, leaving out people, procedures, administration, legal and cultural issues.

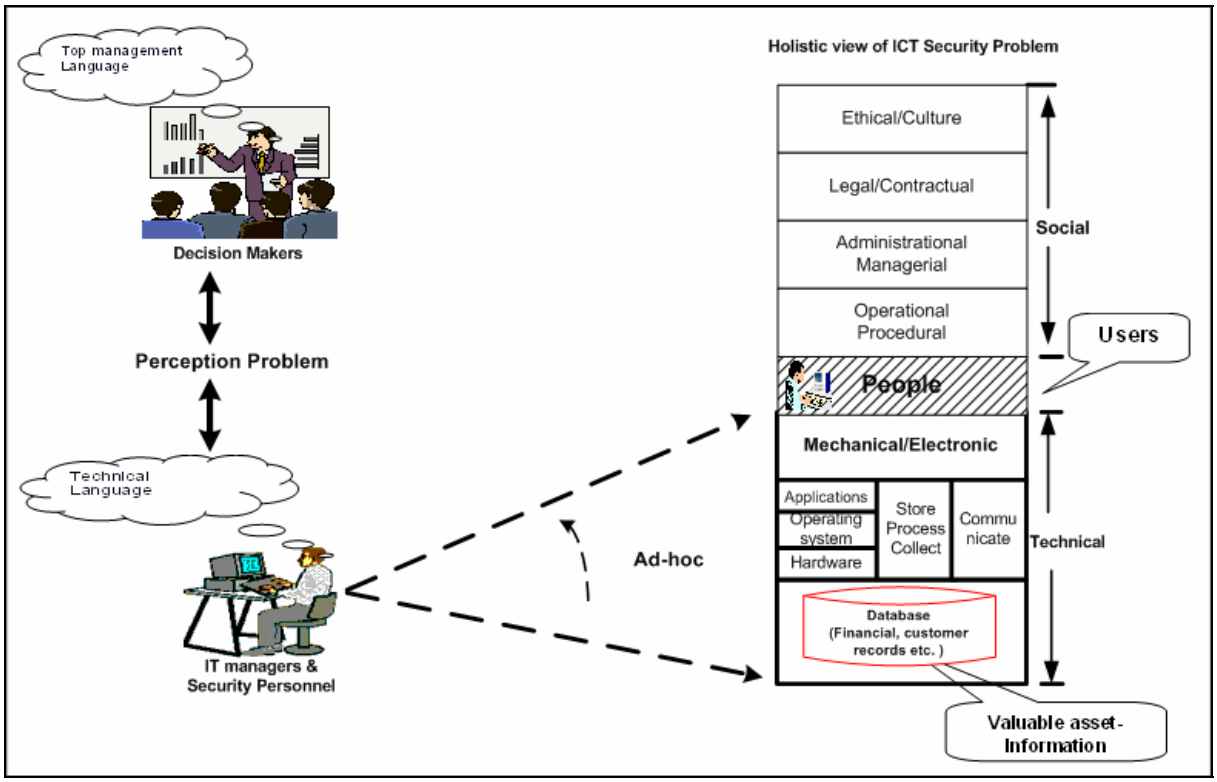


Figure 1: How the ICT Security Problem is perceived and the way is being addressed

Accordingly ICT security problem was perceived by the management as technical problem and not as part of the business risk and for that matter not a part of risk management which in principle is management's responsibility. In this case due to lack of necessary support from management, technical personnel have been addressing the problem on an ad-hoc basis as indicated in the figure. Hence merely the implementation of MSS in such an environment can not meet intended objectives.

5.4 ICT security awareness

Referring to the study, where respondents were asked to rate their computer knowledge and the level of ICT security awareness, 80.9% of the respondents ranked themselves as good or above average in computer knowledge. 70.6% ranked themselves as good or above average in ICT

security awareness. The results also show that about half of the interviewed CEOs are well informed about ICT security problems and the other half were average or below average. However, despite the awareness and recognition of threats by members of the senior management, there are alarming gaps in the organisations concerning ICT security management. There is a perception problem where management merely sees ICT security problem as a technical problem instead of part of the business risk. In such a situation, it is evident that the level of risk associated with ICT is not fully appreciated. Therefore, if ICT security is to be outsourced it will be treated as solely a technical problem, which increases the possibility of selecting inadequate MSSP which may result in even more operational risks, fraud and errors.

5.5 Infrastructure and cost

The lack of appropriate infrastructure to enable an MSSP to offer its services in this part of the world is yet another serious problem. Because of this, the mode of operation may require extra investment on the client and providers side. Firstly, for example, in order to ensure that online monitoring is taking place the power supply to the systems must be reliable, and in the case of the studied environment, the need for reliable backup power generators cannot be overemphasised. Secondly, the MSSP may have to establish their own dedicated data communication infrastructure which may involve the installation of a satellite based systems and purchasing expensive bandwidth. An alternative to online monitoring is the deployment/stationing of technical staff on the client side. In addition, investment in more sophisticated equipment to take care of different version of software such as operating systems (which were for example found to be from windows 98 through to XP, different version of Macintosh, and Linux. would be required. All of these mean additional cost which must be mutually borne by MSSPs and clients.

5.6 Focus is on the computerisation Process

The findings in the studied organisations and the ones observed through other related studies in Tanzania show that the integration of ICT in core business in some developing countries started much later than developed countries (see the dotted lines in Figure 2).

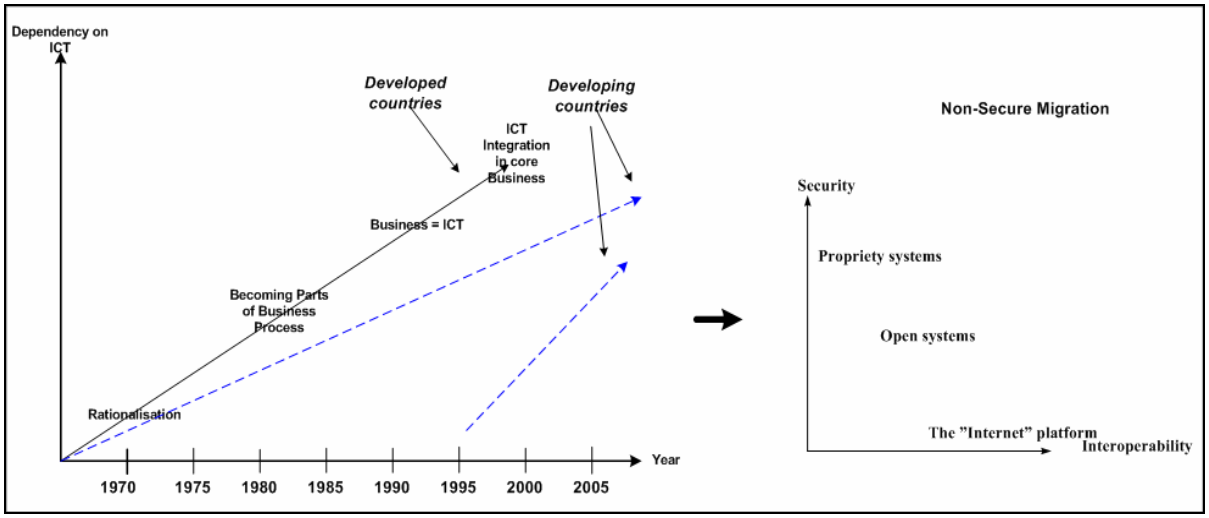


Figure 2: ICT Integration in Core Business vs Non-secure migration (Bakari, J. K. 2005a; Pg. 61)

The gap between the two graphs (the developed countries and the developing countries) indicates among other things the extra work developing countries have to consider both initial

computerisation and at the same time ensuring that the computerisation process is secure. Since more attention is on purchasing/supply and installation of information systems than on use including security, outsourcing of ICT security services will most likely be performed as outsourcing a black box.

5.7 Sense of ownership and trust

When outsourcing, organisation needs to retain ownership and responsibility for the secure operation of the information systems (Allen et al., 2003). Apart from lack of designated internal ICT security personnel/unit in all studied organisations, the sense of ownership in the organisations was yet another problem noted. In such situation, the decision of whether or not to outsource the ICT security service to the third party need carefully approach otherwise further problems can arise. For example in the absence of ICT security personnel/unit, the entire problem might end up being delegated to the provider. In such cases there are many issues that need to be sorted out. For instance, how will the question of trust be handled then? Who will be accountable when something goes wrong on the privacy and security of records containing sensitive client information? When answering these questions, one should also remember that in most cases MSSP use tiered providers (Tiered providers are the subcontractors used by the MSSP and any other downstream subcontractors: Allen et al., 2003 – Page 7). Clearly this is against the whole concept of managing this type of risk.

5.8 Prosecution and other Legal related issues

Not many developing countries have legal framework that supports ICT world and the forensic skills required to support legal proceedings. For example, according to the Legal Reform Commission of Tanzania (LRCT, 2005), the basic commercial laws in Tanzania originated in the 19th century, and most of them were enacted under British Colonial rule before the 1960s (the Ordinances), designed to handle paper-based transactions. Despite the regulatory steps in the laws, electronic transactions such as digital signatures, reforms to contract laws, dispute settlements and others are still not given sufficient attention (LRCT, 2005). Currently the Legal Reform Commission of Tanzania is working on a legal framework that is relevant to the digital age. Until such a legal framework is in place, handling ICT security related prosecutions will be a major challenge, in particular to clients (organisations) who do not have a complete knowledge of the status of their ICT security and to the MSSP who in this case will be offering the services as a "black box" to the client. In the East African Fraud report survey by KPMG, (KPMG,2002) where 82% of the respondents considered their computer and information systems to be a potential security risk, the main reasons for the increase in fraud pointed out by respondents were: lack of adequate penalties and enforcement (53%); inefficiency of the justice system (61%); sophisticated criminals (72%). Furthermore, 64% of the respondents indicated that suppliers are the source of the largest financial losses.

5.9 Termination of Relationship

According to Allen, (Allen et al., 2003), all outsourcing agreements must anticipate the eventual termination of the agreement, and therefore plan for an orderly in-house transition or a transition to another provider should be in place. In addition, outsourcing agreements terminate early more frequently than expected and under circumstances that were not anticipated. This is a big challenge for an organisation which never had in place proper ICT security management before outsourcing its ICT security services to an MSSP. These two points are yet another reason for having well established ICT security management in an organisation as a pre-requisite for the decision to outsource. In the five organisations studied, for instance, none of them were in that position, and the same scenario applies to many organisations with similar state of ICT security Management.

6 DISCUSSION

The end result is to ensure that information systems are adequately protected whether internally or by outsourcing. However, when outsourcing ICT security, organisations are actually giving the service provider access to their valuable asset—information. For that reason, if organisations are to outsource, there are number of issues that need to be addressed. Firstly, they should understand that they are actually transferring one of the most critical risk to a third party, therefore they need to know the magnitude of the risk they are transferring, how critical it is, how are they going to handle the consequences, such as controlling the level of access they grant to their service providers and ensuring that some of their policies such as the way they screen their employees, meet their standards. Secondly, they need to know what procedures should be adopted if the provider fails to deliver.

Generally there is a need to have a detailed analysis at both ends - the provider's end and the client's end. In the case of the studied organisations for example, where ICT security policies and procedures were outdated or missing, the first step after a complete ICT risk analysis would have been the formulation of ICT security policy and procedures, followed by its operationalisation plan.

It is of paramount importance that an organisation carefully evaluates its options and determines whether or not outsourcing is the right choice. However, the process of evaluation requires expertise which is among the challenges to be addressed first if outsourcing is to be considered. After evaluation, the next step is to consider a number of providers to determine which has the expertise to meet the organisation's needs. Another area of consideration is the development of service-level agreements with the candidate MSSP. Service –level agreement implies legal issues and this is one area that might draw critical legal liabilities, because the studied organisations, have no expertise in security matters, they may find it difficult to ensure that the contract/agreement has been formulated in a proper and legally correct manner. Outsourcing MSS have legal implications such as jurisdiction differences in applicable laws and regulations and the law's compatibility between the client and provider. A careful approach is required when preparing agreements in particular when client and provider are in different countries and when deciding how to handle disputes. It is therefore important that legal issues are cleared and agreed from the outset by both parties, in particular in the event of absence of a legal framework for one or both parties (provider and client). If outsourcing is decided, an MSSP has been selected and the organisation's security is being managed externally, it is important to have audit processes in place which are agreed by both provider and client, so that the organisation can monitor the providers' activities and ensure that its ICT security policies and procedures are followed as stipulated in the agreement.

Looking at the outsourcing solution as defined in the discussion above, at least the following pre-requisites must be in place. Firstly, skilled ICT security staff or hired ICT security experts are required to assist the management in overall analysis before reaching a decision on whether or not to outsource. This capability is low in the organisations studied. Similar situation have been observed in other developing countries and in Small and medium enterprise (SMEs) in the developed countries. For example, some SMEs in the developed countries are said to have similar characteristics as those discussed in this study. These are characterised as: having a relaxed culture and without any formal security policies, and a small IT staff with no security training. They face similar challenges, and problems complexities as noted here (Dimopoulos, V. & Furnell, F., 2005). Secondly, looking at the nature of operation/implementation, it requires good infrastructure in place whereby a customer can be serviced remotely. Due to poor infrastructures remote monitoring is impossible; in which case an alternative is for the MSSP to deploy its equipment and staff at the client site which definitely is far too expensive. Thirdly, is the absence of legal framework that supports the ICT world.

Before organisations outsource their ICT security services, they first need to become expert in their ICT related risks, and they need to see the ICT security problem as a 'white box', the capability that is not available for the moment. Outsourcing ICT security is managing ICT-related

risks by transferring the risk to a third party (the MSSP). However, transferring ICT-related risks is not the same as transferring other traditional risks to a third party! The decision makers or managers who are entrusted to manage business risk need to understand that ICT security management is a part of overall business risk management. They should further understand that ICT-related risks are not the same as transferring other traditional risks to a third party but rather a process that needs a careful approach.

In analysing these discussions, given the nature of the problem and the environment, much of the services expected from the provider's end are on the technical side. As discussed under technical implementation, the outsourcing solution means addressing only part of the security problem. The improvement of the social side is more on the organisation itself. Awareness, legal, policy and procedures which were found among the major problems in the studied organisations are not going to be improved by outsourcing ICT security problems to a third party. This is mainly achieved by improving internal processes and therefore a clear indication that the security problem in the studied organisations can not be solved by merely outsourcing the ICT security to a MSSP.

7 CONCLUSION

Outsourcing, which to many organisations/users seems to be an off-the-shelf solution to the ICT security problem, requires some work to be done in the organisation first. Revisiting the advantages and disadvantages of outsourcing in the discussion, it appears that there is a need to have an information security management process in place first of all before one can think of outsourcing. In the digital world information systems are directly linked to the core services of the organisations. This being the case outsourcing security services of these information systems is outsourcing probably the most sensitive risk of the organisation. The management needs to understand the magnitude of such risk in its completeness. As pointed out in the discussion the consequences of mishandling of privacy and security of records containing sensitive client and corporate information can be great to the organisation and which could lead to loss of credibility, loss of customer and staff confidence, loss of market and in some cases go out of business completely.

8 REFERENCES

1. Alberts, C. & Dorofee, A. (2003). *Managing Information Security Risks, The OCTAVE Approach*. Carnegie Mellon Software Engineering Institute, USA. Addison Wesley.

2. Allen, J., Gabbard, D. & Christopher (2003). Outsourcing Managed Security Services. http://www.cert.org/security-improvement/modules/omss/index.html. (Accessed 19th April, 2006).

3. Bakari, J. K. (2005a). Towards a holistic approach for managing ICT security in Developing Countries – A case of Tanzania. *Licentiate thesis, Department of Computer and Systems Science, Stockholm University and Royal Institute of Technology, Sweden.*

4. Bakari, J. K., Magnusson, C., Tarimo, C. N., & Yngström, L. (2005b). *The Mitigation of ICT Risks Using EMITL Tool: An Empirical Study*. IFIP TC-11.1 & WG 11.5 Joint Working Conference, USA: Springer Pp. 157-173.

5. Bakari, J. K., Tarimo, C. N., Yngström, L., & Magnusson, C. (2005c). *State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case study*. The 5th IEEE (ICALT 2005), Kaohsiung, Taiwan. Pp. 1007-1011.

6. Ding, W., Yurcik, W., & Yin, X. (2005). *Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers* Workshop on Internet and Network Economics (WINE), Hong Kong. Also available at http://www.projects.ncassr.org/econsec/wine05.pdf (Accessed 4th June, 2005).

7. IBM. (2004) http://www.ibm.com/ (Accessed 15th January, 2004).

8. Kowalski, S (1994). 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,*

9. KPMG. (2002). East Africa Fraud Survey 2002 Also available at http://www.kpmg.co.ke/ (Accessed 23rd October, 2003).

10. LRCT. (2005). Law reform Programme of Tanzania, http://www.lrct-tz.org/publications.html (Accessed 20th February, 2005).

11. Magnusson, C. (1999). 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*.

12. Sadowsky, G., Dempsey, J. X., Greenberg, A., Barbara J. M. & Alan Schwartz, A. (2003). Information Technology Security Handbook. *Global Information and Communication Technologies Department, The world bank.*

13. Dimopoulos, V. & Furnell, F. (2005). *A protection Profiles Approach to Risk Analysis for Small and Medium Enterprises.* IFIP TC-11.1 & WG 11.5 Joint Working Conference, USA: Springer Pp. 267-283.

PAPER IV

Issues and Challenges to be addressed in e-Government from an Information Security Point of View

Reprinted from

The Proceedings of the IST-Africa 2006 International Conference
Eds. Paul Cunningham and Miriam Cunningham, IIMC International Information Management Corporation
Pretoria, South Africa
03-05 May, 2006
ISBN: 1-905824-01-7

IST-Africa

IST-Africa 2006 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2006
ISBN: 1-905824-01-7

Issues and Challenges to be Addressed in e-Government from an Information Security Point of View

Jabiri Kuwe BAKARI[1], Charles Ndekarisho TARIMO[2] , Beda MUTAGAHYWA[3]
[1,2]*Stockholm University, Forum 100, Stockholm, SE-164 40 Kista, Sweden*
Tel: +46-8-16 1697, Fax: + 46-8-703 90 25, Email: [1] si-jba@dsv.su.se , [2] si-cnt@dsv.su.se
[3]*University of Dar-es-Salaam, Box 35062, Dar-es-Salaam, Tanzania*
Tel: +255-22-240641, Fax: + 255-22-2410690, Email: bmutag@dsm.ac.tz

Abstract: One of the aims of e-government is to apply information and communication technology (ICT) to all aspects of the government's services. In this case members of the public and businesses can benefit from fast and improved administrative processes (public services). This implies relying heavily on ICT to handle a critical part of the nation's information assets. The primary focus is on consistent use of ICT in all aspects of the government's services where ICT can make it possible for it to achieve efficiency, flexibility and effectiveness. However, information security, or in other words the risks associated with the use of ICT, is not receiving the required attention as this development is taking place in some developing countries and in particular Africa. This paper attempts to underline the ICT security problem and its implications for the emerging e-government structures. Given the stage at which most of the developing countries are, with respect to e-government developments (early stages), they stand a good chance of building in security as they develop their e-government systems from the start.

Keywords: E-Government, Information Security

1. Introduction

E-government adoption has led to tremendous changes in the economy and social services worldwide. Examples of these are improved service delivery, reduced corruption, increased transparency, increased revenue and cost reduction [3]. However, in the developing world the introduction and implementation of e-government is still limited and faces a wide range of constraints and challenges [9]. There exist different explanations regarding the nature and causes of the problem. There are those like Massingue [19], who argue that the knowledge necessary for effective use and exploitation is not being transferred at the same speed as the technology itself, while others like Wanyembi [20] attribute the problems to that of a paradigm shift, in that the rapid diffusion of ICT in organisations and governments in developing countries is a new phenomenon, which presents new challenges.

Despite these problems, the dependence on ICT to operate some of the core services of governments and organisations is increasing rapidly. At the same time threats and vulnerabilities to these information systems are also growing. This implies that traditional approaches to protecting information are becoming insufficient as the environment changes to include new methods (ICT) for information and services handling. The goal of this paper is to highlight and discuss issues and challenges to be addressed in e-government from an Information Security point of view. Some understanding as to the nature and characteristics

of ICT security and associated management techniques is required, in order for e-government initiatives to yield the desired results. We believe that, given the stage at which most of the developing countries are, with respect to e-government development (early stages), they stand a better chance of building in security as they develop their e-government systems. Hence knowing and acknowledging the problem from the beginning might help in developing secure e-government systems which in turn would avail the desired flexibility, efficiency, trust, and effectiveness in government services.

The rest of the paper is presented in the following order: section 2 will define and discuss information security problems as applied to ICT. Then e-government processes are discussed illustrated with some case examples in section 3. Information security issues and challenges in e-government implementation are discussed in section 4 of the paper and finally a conclusion is given in section 5. References are provided in section 6.

2. Information security Problem

Before we proceed with the discussion, it is important to define what the information security problem is all about and highlight its status in terms of incidents reported from the early nineties. Information and communication technology (ICT) security is defined as:
"the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document, and counter such threats" [6].

From this definition it is implied that information security covers not just the information, but the entire infrastructure that facilitates its use - processes, systems, services, technology, including computers, voice and data networks. With the current e-government developments in some developing countries, the primary focus is placed on a consistent use of ICT in all aspects of the government's services where ICT can make it possible for it to achieve efficiency, flexibility and effectiveness, while little is being done on the information security aspects involved in these developments. This development trend, if left unchecked, will be a recipe for disaster in the future—imminent computer abuses. This can be projected from the fact that serious computer abuses are increasing not only in the developing world but also worldwide. Figure 1 shows that the problem of insecurity resulting from the use of computers and networks is growing exponentially. While the rate at which new vulnerabilities are discovered continues to increase, the number of reported incidents is also increasing.

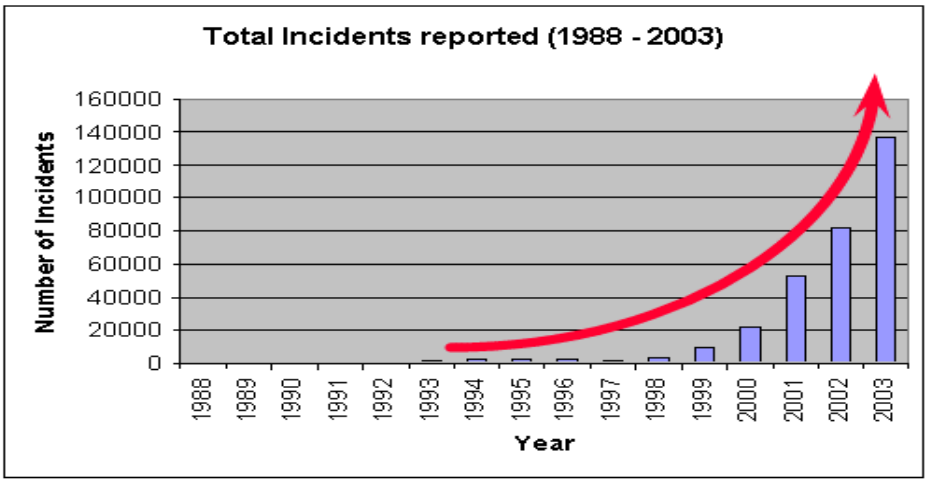


Figure 1: Trend of reported incidents, Source: [7]

ICT security-related cases are increasing and will probably increase further as the computer literacy level in the general public in developing countries and in particular Africa improves. Predictably, for developing countries, it can be assumed that, for every case detected, there are more cases that are unreported and even more undetected [9]. Some of the reasons for this situation are: limited technological knowledge of the majority of ICT users in the environment, lack of ICT security training, poor infrastructure and so forth. As a result, most current implementations are vulnerable to various ICT security attacks, which may have a negative effect on e-government initiatives. One example is the huge sums of money, reported to have disappeared or been stolen through computer fraud [11] in East Africa countries. In the reported survey, about 82% of the respondents considered that the security of their computer and information systems was at risk. A similar problem is reported in [3], where public opinion surveys in various countries place concerns over privacy and security at the top of the citizens' doubts about e-government. This background is used to explain in the next section the e-government process and the ICT security issues involved.

3. E-government Process and ICT Security

There are many definitions in the literature about e-government as discussed in [Gronlund, 2005]. In our case, we consider Gronlund's suggestion of using the Organisation for Economic Co-operation and Development's (OECD) definition which defines e-government as "The use of ICT, and particularly the internet, as a tool to achieve better government". OECD is an international organisation helping governments to tackle the economic, social and governance challenges of a globalised economy. A similar definition is found in [6] which states that "E-Government refers to the use by the general government (including the public sector) of electronic technology (such as Internet, intranet, extranet, databases, decision support systems, surveillance systems and wireless computing) that have the ability to transform relations within the general government (bodies) and between the general government and citizens and businesses so as to better deliver its services and improve its efficiency." This process involves people; hardware which includes computers, networks gadgets; software which includes operating systems and applications systems, systems (which is a combination of hardware, software and people) and most important the information being transacted. This scenario or process which involves people and machines is the one that we are sceptical about and hence try to address in this paper. Without proper planning for security it is hard to: ensure the availability of e-government services and data once in place; protect against disruption and unauthorised interception of communications; ascertain the integrity—that data which have been sent, received or stored are complete and unchanged; provide the needed confidentiality of data; and finally, to provide protection of the information systems against unauthorised access and against attacks involving malicious software and securing authentication.

The overall goal here is to afford individual citizens access to, where possible, all governmental agencies by electronic means in order to obtain the various governmental services independent of time and place. It is not expected, however, that government officials will be working around the clock but some of the services will be available online. This kind of arrangement demands the existence of a reliable communication infrastructure to facilitate the exchange of information within the government, and between the government and citizens. The reliability of this system is partly provided by ensuring its security as explained above. This new technical infrastructure will, for example, be comprised of communication links between different government agencies, security and identification mechanisms, and solutions for provision of long-term documentation. Let us now look at the few cases of what have been considered as e-government initiatives in

some countries around the world [3, 18, 13, 16] and some problems encountered in the course of those developments.

Table 1: Examples of E-government initiatives in various countries

No.	Country	Cases	Description of the initiatives
1	India	Bhoomi system implemented in the state of Karnataka in South India and was launched in all districts of the state in 2001	This system allowed farmers to receive a record of their land holdings at a reasonable price and also enter requests for mutations (changes in the land record resulting from sale or inheritance) into the system. The main product of the system was a Record of Rights, Tenancy and Crop (RTC) certificate that is provided for a nominal price of Rs 15 (about ($0.33) [13]
2.	Chile	Chile's government procurement e-system	This is an e-procurement system used by the Chilean government to buy or purchase goods from the private business sector.
3.	Jamaica	Jamaica customs automated services online	This is a project that modernises and automates customs processes in order to facilitate the procedures for the importation of goods into the islands and the collection of government revenue at the points of entry. The online system is designed to capture entry data electronically by connecting seamlessly to the Customs Automated Services (CASE).
4	Guatemala	Guatemala's Banca SAT ETax Services	This is a system of online filling in tax and payment supported by the World Bank and managed by the Guatemalan Tax agency.
5	Mozambique	e-SISTAFE	A standardised and computerised system for the administration of public finances (State Integrated Financial Management System).
6	Tanzania	Government payroll and Human Resources Information System	Intended to create more efficient management of government employees
7	Cameroon	Tax portal	The site provides tax-related data and guidance for citizens and businesses, information on payment and refund procedures [16]

From these examples, a common theme is that they are all about information systems (land registration, taxation, procurement process, etc.). This involves capturing information at one point and storing, processing, and transmitting it for use at a later stage and in other places.

There is clear evidence that interruption of operations that are based on computers, e.g. systems failures, loss or exposure of confidential data or theft of the computing resources themselves, could lead to failure of the project or initiatives. In addition, depending on the critical nature of the system in question, such interruptions could lead to a major crisis. For example, in the Bhoomi project [13] in India, before the project was implemented the village accountant (or *patwari* in Karnataka) maintained all the records and there was a certain protection of privacy as the accountant would allow only the farmers concerned to see their records. However, there was abuse of this power as corrupt accountants could show the records to anybody for a price, which was not reported anywhere. After the implementation of the project, it became possible to expose potential corruption, such as changes made to records without the knowledge of the record owners. This resulted in some demand-side stakeholders welcoming the ability to view the land holdings of other owners, presumably to detect illegal acquisitions. This however introduced a security problem in that some owners who could not afford the land tax and therefore had not paid it, become targets for land sharks, who were easily able to obtain details about such land and target the

owners. This became one of the major problems of the project as citizen lost confidence and trust in it.

4. Information Security Issues and Challenges in E-government implementation

Several studies [1, 18, 17, 3] agree that e-government in general is a driver for wealth creation and growth, but all acknowledge that there are many challenges which could hinder the exploration and exploitation of its opportunities. This calls for the need to address them at the outset. It is not our intention to revisit all these issues and challenges, but rather focus our attention on those relating to information security.

In addressing the issues, we will use a categorisation proposed by Kowalski in [14], which involves: ethical culture; legal; administrative and managerial; operational procedures; policy and technical issues. ICT security is an attribute that touches upon all of these categories—a multi-disciplinary problem (social-technical) [14], with a social and technical dimension sandwiching the people (user) in between, as shown on the right hand side block (holist view of ICT Security Problem) in figure 2. Hence any efforts to tackle the ICT security problem need to be holistic with respect to the mentioned categories.

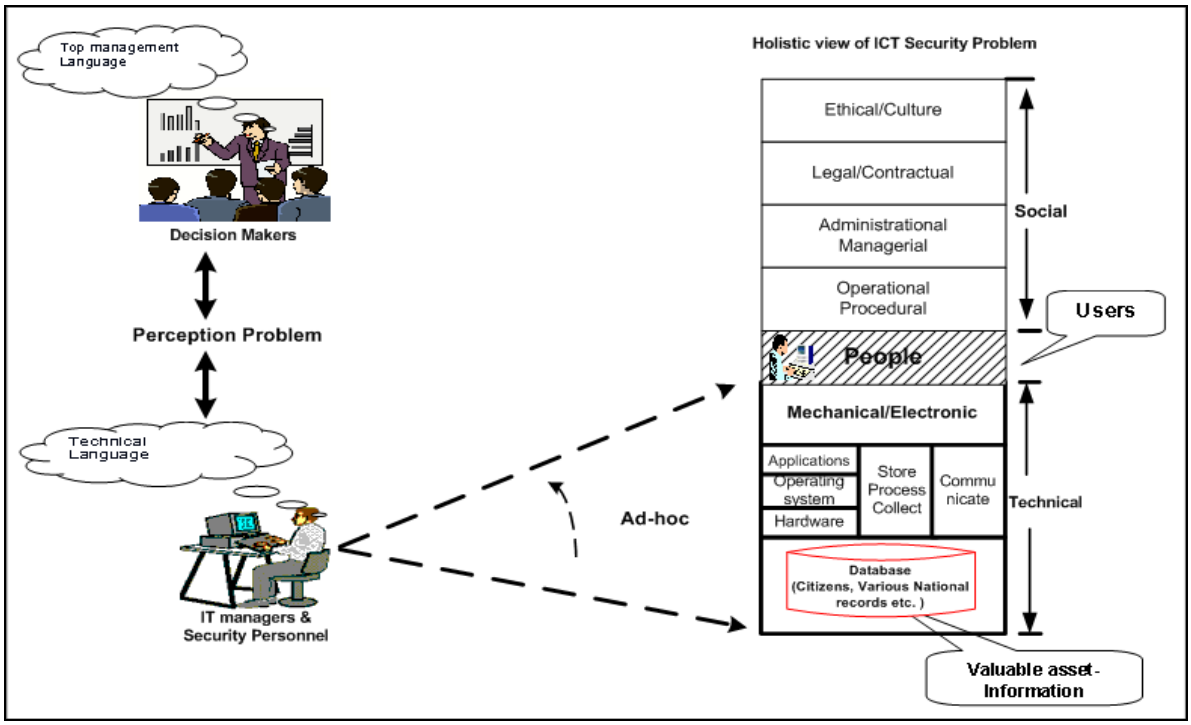


Figure 2: How the ICT Security Problem is perceived and the way it is addressed

As stated earlier, the main goal of ICT security is to ensure that the information assets (various government information systems) are secure. In the figure, we have decision makers (could be principal secretaries in various ministries, etc.) and technical staff on the one side and the holistic view of the security problem [14] on the other. In the figure, users include technical people, managers (those entrusted to operate, manage and maintain the systems), the citizen accessing remotely from home, the Internet café or the e-government system's service kiosk. The information assets could be tax collection and administration process, financial information, and in the case of Bhoomi project [13] for example it was the Record of Rights, Tenancy and Crop (RTC) certificate.

There is a perception problem between the management and the technical personnel as regard to how they view ICT security problem as captured in figure 2. This was a finding of

a recent study on the status of ICT security management in a few selected Tanzanian organisations (mainly government owned) [9]. The findings revealed that the ICT security management problem is being addressed on an ad-hoc basis as indicated by dotted lines. Meaning that, there is a general lack of proper planning for ICT security in place. Based on these findings, we are going to describe the issues and challenges across the categories mentioned at the beginning of this section and relate them to e-government initiatives.

4.1 Ethical/Culture issues

In any society there are controls, one of them being the formal law, which will punish a citizen who breaks it. Where no formal law exists, behaviour tends to be governed by informal laws. These are what we call norms/ethics. Here our focus is on the behaviour of the user, e.g. the citizen in the e-government services' system. User behaviour can cause accidental security breaches, due to a lack of understanding of the implications of one's actions. It follows therefore that the ethics component in computer use in e-government needs to be addressed at an early stage, using well planned ICT security awareness and training programmes and should be a major component of information security efforts. ICT security can be enhanced by the mere fact that people know instinctively what they are supposed to do, rather than being forced somehow by external stimuli. It is important to note that security is only as good as its weakest point and all efforts can turn out to be useless through human error, which results from users not being aware of the risks and not being familiar with sensible and simple security practice.

4.2 Legal issues

"At the centre of it all we have Information and Communication Technology (ICT), not only as a motive force of development and possibilities which the information society affords but also as a factor generating legal problems which have to be dealt with"

[10]

Definitely an e-government initiative would not be complete without a supporting legal framework. Legal issues, in particular computer/cyber crime (a violation of the law committed with the aid of, or directly involving a computer or data processing system), are becoming an indispensable part of ICT risk management. There is therefore a need to be aware of the legal implications in the whole process of e-government and reforms need to be made in the existing legal structures to accommodate the new environment brought about by ICT. For example, it is important to be aware that it is illegal to: gain unauthorised access to a computer system; introduce unsuitable software in IT systems installed for services; use pirated computer software; etc. Continuous legal reform programmes may help to provide the means to control and prosecute such violations.

There are certainly a number of issues that need to be clarified, such as those detailed in [10]. For example, when an electronic document is sent to a public authority or to a private entity, is it deemed to be received according to procedural law or contract law? Will electronic places and electronic handing-over enjoy the same legal protection and legal effects as its traditional physical setup? Another example is that of signature. Everybody knows that it means something special to put your signature to a document. It means that you accept and commit yourself to the contents of the document. It means that you are bound not only legally, but also morally, by the document. When a citizen signs a document and submits it to the government, he is indicating his assent to the contents of the document. The stamp on the document is the government's equivalent of the citizen's signature. While the signature is a symbol of commitment, the stamp could be regarded as the symbol of the impersonal power of government. Such functions of the signature, the stamp and their equivalent, need to be sorted out before a particular service is transferred to

the digital environment where applicable [10]. There are various initiatives being given priority, which developing countries can learn from as far as legal issues are concerned, such as the EU Electronic Signature Directive (EU Directive), and 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 [4] for handling citizen information.

The major challenge accompanying e-government initiatives is the uncertainty as to whether adequate supporting infrastructure is in place, including the legal framework, to sustain these developments and hence avail the benefits to the citizens and the nation as a whole. Important questions to ask before going too deep into deploying e-government systems and services are: does the government, through its various bodies, have the capability to detect, prevent/control, recover from, and prosecute likely ICT-related threats and associated incidents? (This may touch upon the legal system and the police force's readiness.); how about the awareness of the general public concerning their obligations as they interact with e-government systems? Do they know what is legal and what is illegal with respect to their actions? How will the resulting e-government infrastructure be controlled, developed, and secured? There should be a strategy well in advance on how to integrate the individual e-government systems gracefully, say at a ministry level, with other ministries to form the overall infrastructure without compromising the information and systems security. Some of the ICT infrastructure security issues in relation to legal forces are explained in [15]. If answers to these questions cannot be provided at the beginning of a massive e-government initiative, then the sustainability of the project is questionable.

4.3 Administration and Managerial issues

ICT security administration is administering or managing ICT-related security risks. However the use of the words ICT security appeared to be a new concept to most of the decision makers, in that it is considered a technical problem and not a business one. As confirmed by numerous researches, management sponsorship is important in any effort to improve security in any formal social setup and e-government is no different [2]. The challenges have been on how to get the message across. With reference to our findings from the study, the success in addressing these issues begins by bridging the perception gap between the decision makers and technical staff as depicted in Figure 3 below [9, 12].

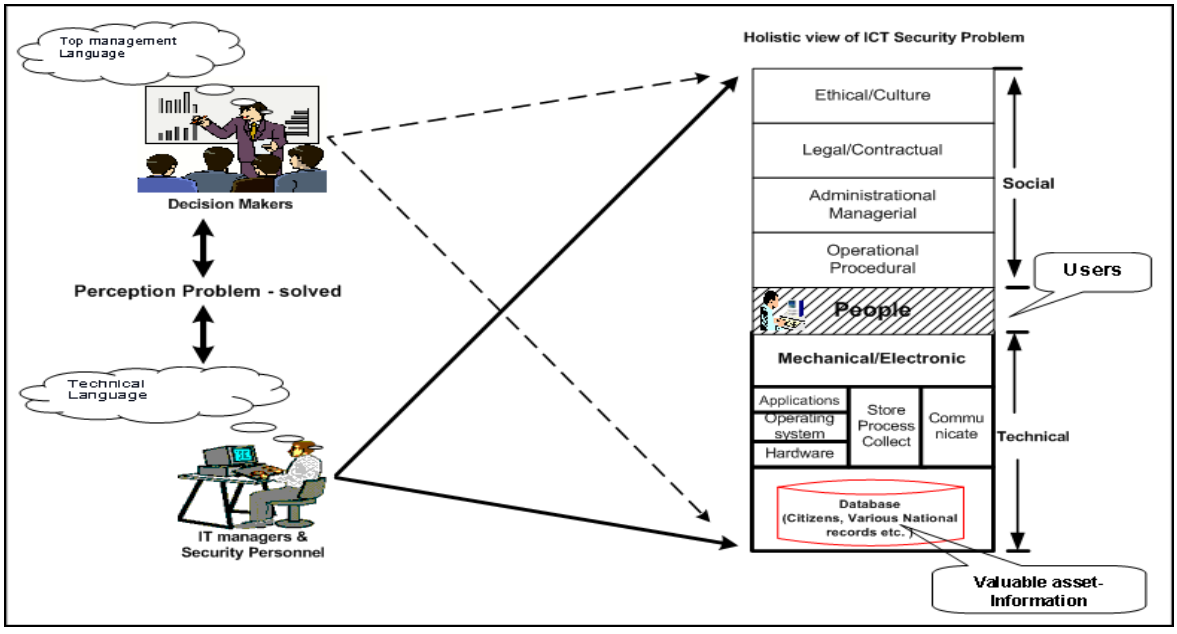


Figure 3: Bridging the perception gap when viewing ICT security problem

Of importance here is how to attain e-leadership and the necessary support at government level while the majority of officials with the power of decision are unaware of the situation as captured in this paper. Government officials will have to understand that ICT risk exposure could lead to e-government service interruptions, direct loss of property and other liabilities, all with great financial implications and which could result in embarrassing media coverage, loss of confidence by citizens and hence loss of credibility in the government [11]. Getting decision makers and government leaders to realise that ICT security problems are part of their responsibility would be an important milestone. If this had been the case, ICT security issues would have featured high on the government's agenda for putting strategies in place for ICT. However this is not what has been happening in practice.

Once the decision makers and government leaders understand the magnitude of the problem, the next important step would be to formulate the strategies on how to go about building a secure e-government. As stated earlier, this is a global problem, and we don't need to reinvent the wheel. There are already a number of initiatives in place in this area. A good example are the eleven principles, adopted recently by the G8, to consider when developing a strategy for reducing risks to information infrastructure and other countries are encouraged to consider them in developing a strategy for reducing risks to critical information infrastructures. The list of proposed principles is also available at [4]. E-government projects by themselves are critical infrastructures but they form part of the information infrastructure and in the eleven principles, information infrastructures form an essential part of critical infrastructures. It is agued that, in order to effectively protect critical infrastructures, countries must protect critical information infrastructures from damage and secure them against attack. It is further insisted that effective protection requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies. Centralised leadership within the government to plan, control and maintain such initiatives is important [5, 8].

4.4 Operational Procedures issues

According to [6] it is easy for government to declare ambitious Internet development plans, but such declarations need to be followed by deeds. One example that we managed to browse through is the Malaysia government at http://www.niser.org.my/. They have what they call the National ICT Security and Emergency Response Centre (NISER) aiming at addressing core ICT security issues in the country. On the contrary, the findings from [9] showed the absence of an ICT security policy at both national and organisational levels, which makes whatever efforts taking place towards ICT security anchorless. Parallel to what we explored in the legal issues, there are many areas to look at in the process itself. For example, traditionally, auditors are used to audit the financial transactions or operational processes and compliances to laws and regulations, policies, standards and procedures. The prime focus for ICT audit is security - evaluating whether the confidentiality, integrity and availability of data are ensured through the implementation of various controls. It also involves evaluating the realisation of benefits to the government from investment in ICT. This implies that there is a need to prepare the government auditors for the process as well, since most of the decisions rely on their opinion.

Another area is human resource. Traditionally, recruitment for the government registry office and other sensitive department/offices used to be special, which meant sometimes getting security clearance. In this era, system administrators need to undergo such a process as they are handling more than the registrars. In addition, roles and responsibilities of individual ICT staff need to be clearly defined.

4.5 Technical issues

ICT security problems are partly technical which could be as a result of software, hardware or network vulnerabilities. In the case of software, there are two fundamental problems, one that affects the application system software and the other that affects the operating system software. Both could be as a result of the introduction of malicious software (virus, worms, etc) or system failure, either due to sabotage or other reasons. In the case of hardware, there could be physical damage, a power problem or the hardware or part of it being stolen. Network security can be a combination of problems that affect both the software and hardware part of the network. It is important to understand that computers, mass storage devices, networks and network components, such as routers and switches, systems and applications software, embedded and wireless devices, and the Internet itself are part of the e-government information systems as is other national infrastructure, such as air traffic control systems, the power grid, etc. A good example would be an improved or computerised revenue authority, which would be made up of all of the above systems and indeed depend on all of the components for its successful operation. Such systems would depend on the physical installation and process of the ICT infrastructure. But again all of this would depend on electric power generation, which in turn relies on a range of ICT systems and capabilities. Today, power companies rely on ICT to collect information about system operation, to help regulate and control power generation, to optimise power production, to respond to changing power demands, to control distribution, and to coordinate the various generation and storage facilities within a power company system, etc. This amounts to a complex system, and so creating an e-government system and coupling it to this infrastructure implies that the coupled e-government system is subject to the same complexities as the total system and that there may be more points of failure than the ability of one to fully comprehend it.

There is therefore a need to plan the infrastructure carefully during implementation, configuration and when purchasing software and hardware in order to assure reliability and security of the proposed e-government systems. Lastly, it is evident that the infrastructure problem in developing countries is not going to end tomorrow. There is therefore a need to keep some of traditional government processes as back-up for some time and, in particular, during the implementation phase.

5. Conclusion

Given the stage at which most developing countries are with respect to e-government development (early stages), they stand a good chance of building in security as they develop their e-government systems. Hence knowing and acknowledging the problem from the beginning might help in developing secure e-government systems/structures which in turn would avail the desired flexibility, efficiency, trust, and effectiveness in government services.

ICT security issues that need immediate attention for e-governments systems implementation have been discussed to some length in this paper. The issues discussed underline the opportunity and fundamental aspects that developing countries and, in particular, African countries have to address in their initial planning and strategies for e-government and other similar projects concerning the use of ICT. These issues also highlight likely areas for further research cooperation between Europe and Africa.

A summary of what is needed to be done at the earliest can be put this way: governments need to have continuous ICT security awareness programmes, whether in the form of training or education in order to sensitise its leaders and people (users) in key security issues of ICT use as highlighted in this paper. Also proper planning for ICT security activities and their achievement in e-government is crucial. This may involve

policy formulation, coordination of security issues at government, or national and international level, as well as contingency plans. ICT security is a crucial issue in any implementation of IT systems for services, and thus this fact needs to be addressed in e-government systems developments that are currently taking place in developing countries. We are now in the information age! Perhaps the introduction of a ministry dedicated to ICT would help to steer ICT initiatives. Such a ministry would then be responsible to coordinate all ICT initiatives in the country. For example, it would put out directives concerning infrastructure, such as the need for new buildings and roads to be e-ready, data communication infrastructures, financial institutions, the oversight of ICT security training at all levels of education, legal framework, and the enforcement of a national ICT security policy.

References

[1] A. Gronlund and T. Horan, Introducing e-GOV: History, Definitions, and Issues. In: Communication of AIS, Volume 15, Article.

[2] B. V. Solms and R. V. Solms, The 10 deadly sins of information security management. In: Computers & Security, Vol.23 No 5 ISSN 0167 –4048, 2004, pp. 371-376.

[3] D. M. West, Global E-Government. In: Centre for Public Policy, Brown University, 2003.

[4] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995.

[5] G. Sadowsky, J. X. Dempsey, A. Greenberg, B. J. Mack, A. Schwartz, Information Technology Security Handbook. In: Global Information and Communication Technologies Department, The world bank, ISBN 0-9747888-0-5.

[6] http://en.wikipedia.org/wiki/

[7] http://www.cert.org/stats/cert_stats.html#incidents accessed 25/02/05)

[8]http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf. (Accessed on 14th November, 2005)

[9] J. K. Bakari, Towards a holistic approach for managing ICT security in Developing Countries – A case of Tanzania', Licentiate thesis, Department of Computer and Systems Science, Stockholm University and Royal Institute of Technology, 2005.

[10] P. Seipel, 'Law and Information Technology Swedish View' Swedish ICT Commission Report, 2002

[11] KPMG, "East Africa Fraud Survey 2002" Also available at http://www.kpmg.co.ke/ last accessed on 23rd October, 2003.

[12] C. 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.

[13] Rahul De, "E-Government Systems in Developing Countries: Stakeholders and Conflict", EGOV 2005, LNCS 3591, pp. 26-37, 2005. Springer-Verlag Berlin Heidelberg 2005.

[14] S. 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.

[15] C. N. Tarimo, L. Yngström, and S. Kowalski, "An approach to Enhance ICT Infrastructures' Security through Legal, Regulatory Influence" The fifth annual ISSA 2005 Information Security Conference in Johannesburg from 29 June to 1 July 2005. South Africa.

[16] http://web.worldbank.org/ (Accessed on 20th February, 2006)

[17] The E-Government Handbook for Developing Countries, A Project of InfoDev and The Centre for Democracy & Technology, The World Bank, November, 2002.

[18] V. D. Ndou, "E – GOVERNMENT FOR DEVELOPING COUNTRIES: OPPORTUNITIES AND CHALLENGES, Department of Business Administration, University of Shkoder, Albania, EJISDC (2004) 18, 1, 1-24.

[19] V. S. 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.

[20] G. Wanyembi & M Looijen, "A Model For Improving ICT Management." Proceedings of the 2000 IEEE International Conference on Management of Innovation and Technology, Singapore, 12-15 November, 2000.

PAPER V

A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards A Culture of ICT Security – The Case of Tanzania

Reprinted from

The Proceedings of Information Security South Africa (ISSA)
from insight to foresight Conference
eds. Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM
Sandton, Johannesburg, South Africa
July 05-07, 2006
ISBN: 1-86854-636-5

A SOCIAL-TECHNICAL VIEW OF ICT SECURITY ISSUES, TRENDS, AND CHALLENGES: TOWARDS A CULTURE OF ICT SECURITY—THE CASE OF TANZANIA

Charles N. Tarimo[1], Jabiri Kuwe Bakari[2] Louise Yngström[3], and Stewart Kowalski[4]

Department of Computer and Systems Sciences (DSV), Stockholm University/KTH

Forum 100; 164 40 Kista, Stockholm- Sweden. Tel: +46 8 6747233, Fax: +46 8 703 9025

E-mail: {si-cnt[1], si- jba[2], louise[3]} @dsv.su.se; stewart.kowalski@ericsson.com[4]

ABSTRACT

This paper discusses the human dimension in a 'security chain' within information systems and networks. This dimension is often overlooked at different stages and levels of ICT development and implementation. An example of this omission could happen at the stages of design and implementation of various ICT systems or strategies and policy formulation concerning ICT use; at the level of an organisation or a country as a whole. As a consequence, this human dimension then forms a weak link in the overall ICT security chain. A common insight in this respect is that, a chain is as strong as its weakest link.

A security chain involves coordinated measures both technical and non-technical (social-technical) necessarily taken to enable the provision and maintenance of adequate levels of ICT security within organisations or a nation as a whole. Several studies in the literature have shown that a supportive security culture is an important component in this chain. Security culture encompasses all socio-cultural measures that complement technical security measures. This paper will, drawing on available literature, attempt to identify and characterise the building blocks of a secure ICT environment in an organisation. The identified building blocks consist of: — people, ICT security requirements, ICT security culture, and security systems. Focusing on people, a discussion of the interaction between these building blocks in a social-technical context is provided based on some concepts from specific theories of Organisational Behaviour (OB). The building blocks and their interactions are then organized into a primary model.

In order for an organisation to create, maintain and change its ICT security culture, certain enabling factors and changes at the national level are instrumental and necessary. Taking a social-technical context of Tanzania, the developed model is used to highlight and analyse some of these factors and needed changes in the light of some collected survey data. In particular, the current trends of ICT developments with respect to security and a supporting human capital are analysed. Further, recommendations of future strategies for ICT development in the country with respect to ICT security are also provided. This paper constitutes a part of an ongoing research from which we present some results.

KEY WORDS

ICT security culture, Security system, social-technical model, awareness, knowledge, attitude and behaviours.

A SOCIAL-TECHNICAL VIEW OF ICT SECURITY ISSUES, TRENDS, AND CHALLENGES: TOWARDS A CULTURE OF ICT SECURITY—THE CASE OF TANZANIA

1 INTRODUCTION

The human dimension is an important component in any security implementation effort. Mounting evidence (DTI, 2004; Ernst and Young, 2004) continue to suggest an existence of significant correlations between observed number of security incidents and people's attitude and awareness of security issues. This observation may imply that, the human dimension in ICT security could be fairly addressed by a cultural approach, that is, by instilling a security culture through security awareness, knowledge and skills. This implication conforms to the assertion that, an effective security culture represents one of the necessary foundations for information security management, and cannot be achieved without appropriate attention to security awareness, training and education for all ICT users (IFIP SEC, 2006). The International Federation for Information Processing (IFIP) Working Groups 11.1 (Information Security Management) and 11.8 (Security Education) have dedicated a special workshop session with a theme on security culture, to be held during the IFIP SEC 2006 conference. Additionally, in the recent years themes on security culture have had almost a permanent place in many of the regular security conferences.

For security to be effective, it takes more than having the state-of-the-art technical controls in place. Effectiveness of security depends also on the extent to which every system user understands and accepts the necessary precautions to counter security threats. Literature suggests three key components that should be addressed in any effective security implementation—people, process, and technology (Schneier, 2000). That is; the *people* involved, the organisation of the *process* involved in securing systems/environment and the *technology* used. Security knowledge and skills of people are very important elements as they help them to act appropriately. But security knowledge and skills without an organised environment in which to apply them is mostly ineffective. The same applies to advanced technology; without an organisational framework, it cannot be fully effective. This paper will, drawing on available literature, attempt to identify and characterise the building blocks of a secure ICT environment in an organisation. The identified building blocks consist of: people, ICT security requirements, ICT security culture, and security systems. Focusing on people (human dimension), a discussion of the interaction between these building blocks in a social-technical context is provided based on some concepts from specific theories of Organisational Behaviour (OB). The building blocks and their interactions are then organized into a primary model which can act as 'an organisational framework' showing ICT security culture in relation to other ICT security controls.

In order for an organisation to create, maintain and change its ICT security culture, we take the stand that certain enabling factors and changes at the national level would be instrumental and necessary. Taking a social-technical context of Tanzania, the developed model is used to highlight and analyse the current trends of ICT developments in Tanzania with respect to a supporting ICT security human capital. In the light of some collected survey data, analysis of the current trends in provision of awareness, training and education programmes in key areas of skills formation critical to sustained development of ICT security knowledge/culture in the country is performed. Discussion as regards to the observed situation and recommendations of future strategies are provided. This paper constitutes a part of an ongoing research from which we present some results.

The rest of the paper has the following sections: Section 2—Background and Rationale of ICT security culture. Section 3—Methodology. Section 4—A discussion of issues related to

security culture in a social-technical context. Section 5 –Findings from survey data in relation to ICT security awareness and knowledge. Section 6 –Conclusions; and References are found in Section 7.

2 THE BACKGROUND AND RATIONALE OF ICT SECURITY CULTURE

There exist different definitions relating to the word culture depending on the context of its application. Generally speaking, it refers to patterns of human activity and the symbolic structures that give such activity significance. Different definitions of culture reflect different theoretical bases for understanding, or criteria for evaluating, human activity. Culture, taken in its wide ethnographic sense, is that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and behaviors acquired by man as a member of society (Cohen, 1995).

Relating the definitions above to the context of this paper, the following two concepts are more relevant—*patterns of human activities* and *the symbolic structures supporting them*. Patterns of human activities in this regards are captured by the contemporary global trends where humans are persistently striving to employ ICT in all social-economic-cultural activities. Whereas the corresponding symbolic structures are such as: national ICT policies, ICT infrastructures, general ICT knowledge, specific ICT training programmes, ICT training institutes, and so on. Some of these structures may manifest themselves at the level of an organisation; for example an organisation's ICT policy or organisational culture; whereas other structures manifest themselves at the nation level; for example, the mentioned national ICT policy. Thus, ICT security culture as conceived in this paper has both: *patterns of human activities related to it* and *symbolic structures supporting them*. The focus in this paper is exclusively on *symbolic structures supporting* the ongoing ICT deployments.

Following from the discussion above, it is apparent that culture can be influence by both; factors within an organisation boundary, as well as factors beyond the organisation's boundary. That is, culture is influenced by internal as well as external factors. Before the advent of ICT, it was possible for an organisation to attain security even for information by combining solid/physical access controls, and procedures and processes; as the organisation was regarded as bounded. Unfortunately, this traditional setup of a bounded organisation does not work so well in the current information technology era. This is due to the fact that bounded organisations become unbounded through interconnections and networks. Consequently, the underlying culture of 'security by physical access control' also needs to be changed.

As noted in numerous literatures, cultures are complex and therefore changing them is difficult in most cases (Detert et al., 2000). Within ICT security, culture change involves much more than implementing technology (technical controls) and developing a policy. While technical security controls for ICT systems are critically important (Bishop, 2003; Pfleeger, 2003; Schneier, 2000), they largely depend on the people who operate and come into contact with the systems in their daily duties. The extent to which these, be it systems administrators or regular users, are motivated, knowledgeable, trained, and show willingness in performing their duties with security consciousness makes an important difference. Our focus here is on aspects of motivation, training, skill sets development, and the general knowledge required to foster ICT security culture in organisations and the nation.

The literature holds a lot of information on importance of, and approaches to attain a culture of security with regard to ICT. Example of the available literatures that may be helpful in building a security culture in ICT is the publicised OECD (Organisation for Economic Co-operation and Development) document—Guidelines for security of information systems and networks: towards a culture of security (OECD 2002), which gives high level guideline descriptions for participants at international, national and within organisations. These guidelines constitute a foundation for work towards a culture of security. Conolly (2000) points out that, organisations must have a culture that

makes it clear that security is important; whereas, Verton (Verton, 2000) underlines the importance of security awareness in building organisation's security culture.

Freeman and Wood noted that the body of research is rich in knowledge in the area of organisational security, which addresses aspects such as its construction, and how to improve and maintain it. However, most of the research in this area is focused on certain aspects of security such as security leadership, policy issues, awareness and training, and implementation of specific controls; and not on how these aspects are affected by and could be integrated into, an organisational security culture (Freeman, 2000; Wood, 2000). While these aspects are all very important, their application in organisations requires an existence of some kind of intrinsic support from all participants. This support need to be reflected in, and built upon the organisational culture. Chia argues that the enforcement of an aspect like policy through the traditional cycle of awareness, training, and compliance testing without a supporting culture is likely to be less than optimal (Chia, 2002).

A common theme that can be drawn from the literatures above is that of necessity and importance of security culture in ICT. This necessity seems to be global in nature (OECD, 2002) and it needs the requisite attention at all levels and from all participants (computer systems and networks- users).

The questions here can rather be:

1.) How can participants in ICT meet demands for a sound ICT security culture?

2.) What are the key factors contributing to it?

3.) What are the components of an ICT security culture?

While it is not possible to provide comprehensive answers to all these questions in a short paper like this one, an attempt is made to provide (at least at high level) discussion of key issues with regard to the posed questions. Nevertheless, an obvious general answer for these questions has to do with aspects of awareness and knowledge of ICT security issues as has been revealed in the preceding part of this paper. Also, further relevant and complementing information about culture change and analysis can be found in (Schlienger and Teufel, 2003).

Taking Tanzania as one of the participants in ICT, the current status and efforts (*symbolic structure supporting acquisition of ICT security awareness and knowledge)* towards a culture of security is analysed. This paper can then serve a purpose of country case study and experience towards the goal of global ICT security culture.

3 METHODOLOGY

Being a part of ongoing research, this study is based on primary data sources collected in Tanzania. It is mainly a primary research that involves collection of data (survey data), organising it in some fashion (a social-technical framework) based on some factors (awareness, knowledge, and skills) that we believe are important in fostering ICT security culture. At the level of organizations; six training institutes offering computer/ICT training and education in the country are involved; where their training and education materials/programmes are scrutinized for aspects of ICT security content. Here, the training institutes are regarded as *symbolic structures*. A criterion for selection was to include institutes with training and or educational programmes on computer/ICT. The prime target was on institutes whose programmes are exclusively on computer/ICT training/education. These were complemented by others institutes/university whose curricular include computer/ICT studies in parallel with other fields. At the national level, strategies and policy documents regarding education and training were obtained for reviewing.

The collected data was then analyzed to unveil some trends or pattern, which are then compared against some known examples of good practice in fostering security culture. The primary data sources are, in addition, complimented by secondary data sources from the literature.

3.1 Theoretical basis

A major premise here is based on the belief that, by providing appropriate ICT security knowledge to ICT users, it is possible to internalise security culture. This knowledge could be in the form of education, general awareness of, or specific skills in, ICT security issues. Theoretically, the study is based on the General Systems Theory whereby we view 'system' as one whole (Yngström, 1996), implemented by the social-technical framework (Kowalski, 1994). In a perspective, we view an organization as a social setting with unique cultures, structures, methods and machines. These together can be viewed as constituting a system—*social-technical system*. The social subsystem; has *culture* and *structures* as components, whereas the technical subsystem has *methods* and *machines*. These components are in constant continuous interaction with each other to maintain the system in equilibrium. Thus, changes in any of component or subsystem will tend to effect changes in all other interacting components so as to place the system in equilibrium/disequilibrium.

From the General Systems' theory point of view, *fig. 1* shows a social technical system whereby ICT is being introduced in the technical sub-system (Machines and Methods). Following this change, transformations need to take place in order for the system to accommodate the changes brought about by the newly introduced ICT and once again maintain itself in equilibrium. This study has focused on these transformations from a systems' security point of view. The overall goal is to study, analyze and establish the systems' security readiness requirements taking into consideration the pertinent social-technical states. For the purpose of this paper, an analysis of an aspect of *structures* in the social subsystem—training and education modules targeting ICT security, is on focus.

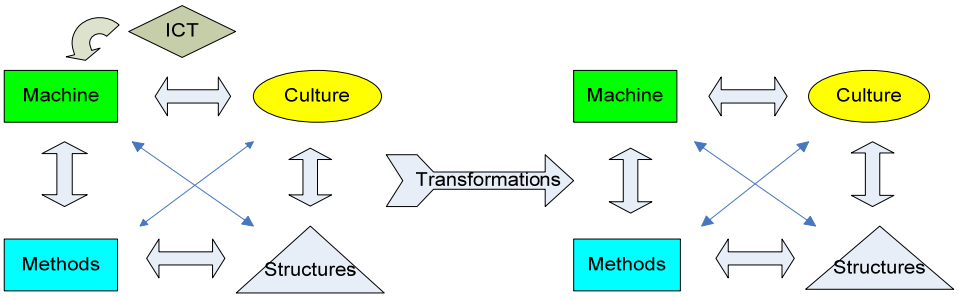


Figure 1: Social-technical system (Kowalski 1994)

4 SECURITY CULTURE ISSUES IN A SOCIAL-TECHNICAL CONTEXT—A DISCUSSION

This section attempts to draw a big picture of ICT security culture in a social-technical context and highlights issues pertaining to the possible answers to these questions: "*How can participants in ICT meet demands for a sound ICT security culture? What are the key factors contributing to it? What are the components of an ICT security culture?"* posed earlier.

Generally, cultures are based on a set of shared underlying assumptions about reality (Robbins, 2003). Here our reality is to attain ICT security in a social-technical system (see fig.1). Culture has effects on attitudes and belief, which in turn play part in individual behaviours—actions and/or reactions. Thus, there is a prime need to determine what attitudes and beliefs need to be cultivated in an organisation, how these manifest themselves in the behaviour of the concerned people and how desirable attitudes and beliefs can be imprinted into formal operational methods to produce the desired outcomes—secure systems, networks, and operations. Thus behaviour needs to be influenced in some ways.

We would like to borrow knowledge already available in other fields in relation to behaviours and attitudes. To this effect, we have found a number of relevant theories from the field of

Organisation Behaviours (OB). Mounting evidence from research in OB (Robbins, 2003) has shown that it is useful in developing people skills; the same should be true for ICT security skills. It is further claimed that actually OB is capable of providing means to explain, predict, and control human behaviour.

Some of the basic theories in OB which could influence behaviour are the following: ***motivation theories***—basically, people are not cold unfeeling machines and hence the theories propose that individuals are motivated to the extent that their behaviour is expected to lead to a desired outcome. Their perception and calculation of situations are filled with emotional content that significantly influences how much effort they exert. Moreover, people who are highly motivated in their jobs are emotionally committed (Robbins, 2003); ***goal-setting theory***— states that intentions expressed as goals can be a major source of work motivation—a potent motivating force; ***reinforcement theory*** – a behaviouristic approach, which argues that reinforcement conditions behaviour; ***law of effect***—behaviour is a function of its consequences and showed that reinforcers (consequences) conditions behaviour and help to explain how people learn.

The law of effect and the concept of reinforcement also help to explain motivation. A large amount of research indicates that people will exert more effort on tasks that are reinforced than on tasks that are not (Stajkovic and Luthans, 1997; Luthans and Kreitner, 1984). Reinforcement is undoubtedly an important influence on work behaviour. What people do on their jobs and the amount of effort they allocate to various tasks are affected by the consequences of their behaviour. Same effect can be produced through goals. This background can equally be used to inform and address the human dimension in security within organisations; as the human dimension in security has to do with behaviours and actions too.

These theories as outlined above point out the following important issues for influencing human behaviour: motivation, goals, reinforcement, and the nature of consequences following an action. In the absence of all these, it seems people may feel themselves being treated as cold unfeeling machines, a condition that could result in adverse effects on behaviours. It is therefore productive if the advantage of these issues can be taken when addressing human issues in ICT security, i.e. to influence the desired behaviours conducive for attaining secure ICT environments in organisations. The desired behaviours would have their roots deep in a vibrant ICT security culture. In order to see how behaviours are related to the overall process of securing an organisation's ICT environment, ICT security culture is placed in a context and then involved actions and issues are outlined. This is the topic of next subsection.

4.1 ICT Security culture in a context: — An overview of parts, relations, and actions

As mentioned earlier, ICT security problems may not always be wholly technical or wholly social but mostly a combination of the two. This combination is realised through the relations and interactions of the social-technical system so formed. Thus, technical solutions alone may not, in the long run, solve the problem. It is from this observation that the concept of security culture finds its relevance in the social aspects of security. Here we attempt to characterise the parts and relations.

According to a common view, information and communication security can be expressed using the three concepts of confidentiality, integrity, and availability. In practice these are afforded through technology, management, and social elements. Technology elements may involve a combination of cryptography, intrusion detection systems, access control mechanisms, firewalls, antivirus, and so on (Pfleeger, 2003). Management elements can be access control policy or a general security policy, procedures and practices. Social elements involve, in addition to the management elements,—ethical/cultural, and legal/contractual issues (Kowalski, 1994). These elements can be grouped into two major categories of technical and social controls.

The actions involved in the process of securing an ICT system requires the knowledge of the possible risks pertaining to the systems, available countermeasures or controls and how to

holistically address them. This may involve analysing the ICT system in question—profiling the would-be adversaries—their intentions, attitudes and characteristics i.e. thinking like hackers; designing countermeasure e.g. developing a security policy, implementing access controls mechanisms, physical protection, and supporting procedures. Normally, this is constructed in layers—deterrence and prevention; protection; detection and containment; and recovery. These layers of controls are hereby denoted as a *security system* and are expected to work harmoniously. A *security system;* is made up of a threat profile from a risk analysis, corresponding countermeasures and needed structures (technical and non-technical)—e.g. secure hardware and software, policies, processes and procedures; (but these lower level details will not be covered here).

However, a *security system* can only be effective not because of its comprehensiveness but also due to the attitudes and behaviours of the people that interact with the system. Thus, the actions of these human elements determine whether the information system in question will be reasonably secured or insecure (assuming a perfect *security system*). This makes *people* an important part of the security system and the OB theories discussed earlier have relevance here. For example, imagine an organisation has in place a good *security system* with a policy that stipulates that all sensitive information from the organisation must be sent encrypted. However, since not all information may be sensitive at any given time, then the system must also have a capability of sending insensitive information unencrypted (in clear). Then, through the actions of a person (attitude and behaviour), this capability can also be used to send sensitive information unencrypted as well, and thus renders the encryption security function ineffective. As attitudes and behaviours are the direct product of the pertinent culture, then cultivating a desired *ICT security culture* is just as important as having in place the right technical controls. Thus, *security culture* is equally an important part of the whole.

The overall range of *security requirements* for an organisation determines the nature of *ICT security culture* that is to be cultivated. In addition, the same *security requirements* determine the policy and types of countermeasures (*security system*) to be implemented. Furthermore, the *security requirements* impose demands on the *people* who would interact with the system. The issues of motivation, training and education outlined earlier are important here also. These different parts or building blocks and relations are shown in *fig. 2*.

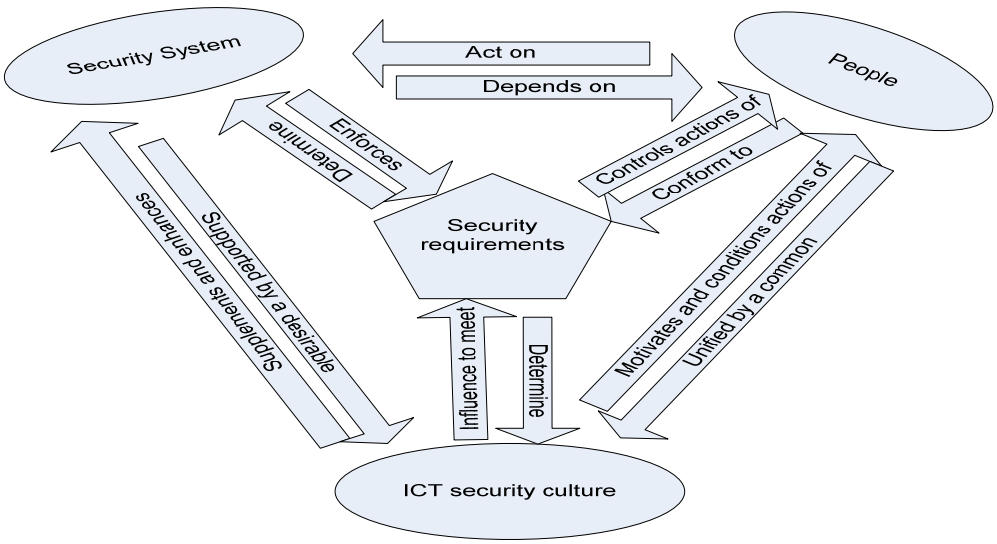


Figure 2: An organisational framework showing ICT security culture in relation to other ICT security controls.

The main issue in focus in this discussion is the behaviour of people. If there could be a method to understand and predict the behaviour, then it's more likely it could also be controlled. As discussed earlier in this paper, at least we have seen OB theories may provide mechanisms for influencing human behaviour. A number of methods can be used to achieve this; such as effective leadership, adequate planning, setting goals, motivating, enforcing responsibility and liability, continuous awareness programs, security education, and imparting security skills.

Cultural aspects in the *fig. 2* can be divided into *security culture mechanisms* (management, policies, personnel, and training and education); *principles and values* (responsibility, honest, integrity, ethics, commitment, compliance, leadership, and motivations), and *shared underlying assumptions* (knowledge of threats and vulnerability in systems, trust relationships, beliefs, and possible malicious acts). These aspects can be realised by breaking the framework, *fig. 2*, to the next lower level to see details of the components; for example the details of the contents of *security system* provided in the discussion above.

Referring to *fig.2*, insecurity in the ICT environment of an organisation could then be as a result of a flawed security system or security requirement specification. Insecurity could also be caused by unwanted actions taken by people due to the absence of a security culture or lack of awareness and knowledge of security issues. As mentioned earlier in this paper, for security to be effective, it takes more than having the state-of-the-art technical controls in place. Effectiveness of security depends also on the extent to which every system user, understands, and accepts the necessary precautions to counter security threats. A security aware culture is one whereby users are aware of the security issues that pertain to their environment, and are knowledgeable and skilled enough to act appropriately.

Thus, based on *fig. 2,* a culture that perceives ICT security to be a technical issue is unlikely to be effective; as in effect, it would only be benefiting from the effects of the *links* and *relations* between the *security system* and the *security requirements*, while missing the-all-important other links and relations shown in the figure. Here, it's where ICT security is represented in a simple equation which says: "ICT security = firewall, or intrusion detection system, or an antivirus, or a combination of the three". Worse still, is where the ICT security in an organisation has a clear and single owner—belongs to IT department! It would also means that this is not an issue that concerns the organisation's top management; their support, which is needed for enforcement of policies, allocating budgets, training, etc., will be missing and hence the whole effort turns out futile.

The culture that tends to address the ICT security problem in an ad-hoc and reactive manner is ineffective, at best; as it misses the big picture as captured in *fig. 2*. Here it's where an organisation responds to security only when there has been a major catastrophe to its processing/IT systems; e.g. an unavailability of systems following a virus outbreak or other possible risks in ICT. In addition, due to lack of proper planning, and the entailing limited and constricted view of the security problem, it's unlikely that the organisation would have a security policy to guide its security efforts; or a proper security awareness and training programmes for its employees/users; which, as discussed earlier, are important in creating and instilling a desired ICT security culture in the organisation and among the employees.

Consequently, the human element in the overall effort of creating a secure ICT environment in an organisation needs to be given the priority it deserves. Desired attitudes and behaviours with regard to security, expected to be displayed by the *people* interacting with information system needs to be cultivated—through awareness and knowledge, motivated, and encompassed within an overall organisational culture; for which a *security culture* could be a subculture. The proposed framework (fig.2) could be helpful in viewing the big picture—a 'whole, with its parts and relations.

In order for an organisation to create, maintain and change its ICT security culture, we take the stand that certain enabling factors and changes at the national level are instrumental and necessary. As discussed in section 2, culture is represented by—*patterns of human activities* and *the*

symbolic structures supporting them. Further it was revealed that these two aspects could manifest themselves at different levels and contexts. Beyond an organisation level, is a national level; and in relation to this, the corresponding *symbolic structures* are such as; national ICT policies, ICT infrastructures, general ICT knowledge, specific ICT training programmes, ICT training institutes, and so on. Following from our stand, a high-level investigation of the extent to which ICT security awareness and knowledge is being addressed in the social-technical context of Tanzania was performed in a search for further insight into understanding the factors effecting the human dimension (*people* in *fig. 2*) in security. This is covered next.

5 FINDINGS FROM SURVEY DATA IN RELATION TO ICT SECURITY AWARENESS AND KNOWLEDGE

The colleted data (see section 3) was organised to indicate the status and trends of the training and education programmes that are on the offer to the general public based on vendor-neutral ICT security training and education programmes. The aim was to find out whether the currents trends of ICT knowledge dissemination involves ICT security knowledge, which as we have seen in the preceding sections, is important in fostering ICT security culture.

Two computer training institutes, one university, one institute of technology, and one regional management institute, and one institute of accountancy were included in the survey. The training/education programmes documents were obtained from these and analysed for the patterns described above. *Table 1* shows the mapping of "other" or "non-security" computer/ICT courses/modules offered by the surveyed institutes and university against security courses/modules, i.e. whether they include security modules. A tick in the cells shows what is available for offer at different course levels.

Table 1: Overview of ICT security courses among a full range of other Computer/ICT courses on offer

Course level	Certificate		Diploma		Advanced Dip.		Degree		Postgraduate	
	Others	Security	Others	Security	Others	Security	Others	Security	Others	Security
Institutes										
CT1	√		√		√					
CT2			√		√		√		√	√
IT			√		√					
IM	√	√								
IA	√				√	√				
UN	√						√		√	

Key: CT1 and CT2 are the two computer training institute; IT = institute of technology; IM = the regional management institute; IA= institute of accountancy and UN= university.

5.1 Discussion

As can be seen on the table, there are only three occurrences of courses or modules bearing ICT security issues among the wide range of IT courses offered by the surveyed institutes /university; one at certificate level, one at advanced diploma level and the other at postgraduate level. This is relatively a small proportion, content wise and out-reach when compared to the other courses in computer/ICT represented in the table. While the other ICT courses have almost occurrences in all levels of certificates, i.e. from certificate level to postgraduate when all six institutes are combined; ICT security courses appear only at certificate, advanced diploma, and at post graduate level; and

this is only in two institutes out of the total six. Still, on looking at the details of the ICT course on offer at post graduate level, it turned out to be an intensive short duration course taking only three week to complete. The contents are: "Overview of IT Developments, Security threats, advanced risk assessment methodologies, advanced issues in Network and Data communication security, Risk matrix and control spreadsheets, Formulating IT Security policies and Data protection acts, total computer security and control in an organization. Whereas, the target group is: ccomputer - based information system managers, Data Processing/Operations Managers, Data-base administrators, analysts/Programmers, auditors and End users who are responsive for preventing, detecting and controlling disruptions, destructions, disasters, and un-authorised access to computers and information systems. While this has positive effects, but the fee for the three week course is on the higher side compared to other non-security IT courses. The fee for this one is US$ 1800 compared to, between US$ 100 – 500 for different modules of most of other IT courses at that level and for that duration. This could be another factor strong enough to keep many of the prospective attendees away.

Other IT courses are various and some are based on international syllabus, whereby local institutes run the courses through accreditation arrangements with external universities, mainly in the UK. Examples of courses are: International Diploma in Computer Studies (IDCS), Bachelors in Computing and Information Systems (B.Sc), and International Advanced Diploma in Computer Studies (IAD).

Since there is a low representation in courses on ICT security compared to others, it may imply also that the competency and awareness of security issues in this social-technical context is relatively low. This assertion is supported by the findings of another study on the state of practice ICT security management in organisations in which the studied organisations rated low in many of the key issues required for a sound ICT security management practice (Bakari et al., 2005).

5.2 Challenges

Although there is a policy at the national level; the National higher education policy of 1999, there are still some operational problems and challenges. Demands for personnel with higher education background have been on the increase both from the public and private sectors. There has thus been a mushrooming of training centres and institutes to cater for the increased demand. The mushrooming of such centres and institute appears to have been haphazardly (encouraged) without proper co-ordination and planning.

Tanzania's education system has grown from relatively simple to a complex one. The system has grown from only one higher education institute (a university college) in 1961 to more than 140 tertiary training institutions; out of which about twenty (20) are higher education institutions. However, many of these have been duplicating one another course programmes and awards (NHEP, 1999). This lack of planning and coordination may also explain the observed discrepancy in the course offered in computer/ICT studies. Most of the institutes offering training and education in computer/ICT studies are private; at times they seem to be driven by the prevailing market forces. Hence there are courses that would attract many students, and these will be honoured accordingly. It appears (from the findings) that, on the one hand there are far more people who want to learn how to use computers and acquire skills on how to use different application packages than those who would want to acquire ICT security skills. Yet, on the other hand; due to inadequate planning as generally noted in (Bennell et al., 1999; Rutayuga et al., 2004) it seems no serious attempt has been made to ascertain that the prevailing labour market demands (including skills in ICT security) for both pre- and in-service training are met. Hence the IT/ICT training provision on offer is essentially supply-driven. The lack of personnel and resources to support information security education at colleges and universities can be another reason. For this deficiency, the lack of trained security experts is a result; which also explains the lack of ICT security culture.

Hence there is an obvious need for cultivating and enforcing ICT security culture. This is an issue that calls for participants at different levels within the organisations and the nation if it is to turn out a success.

6 CONCLUSION

This paper has attempted to address the human dimension in the process of developing, implementing, attaining, and managing ICT security in organisations and/or a nation by reviewing and discussing varying aspects related to building a security culture in ICT. Security culture encompasses all socio-cultural measures that complement technical security measures. In connection with this, issues of attitudes, behaviour, actions, and motivation as they relate to security have been analysed by concepts from the field of organisational behaviour. An organisational framework portraying components of a supposedly secure ICT environment in an organisation has been outlined and discussed. The roles of awareness and knowledge of, and skills in - ICT security issues towards a culture of security have been emphasised in the discussion and this was further supported by analysis of some data collected in a primary research conducted in Tanzania.

In conclusion the following is apparent—cultivating ICT security culture is neither simple nor easy. Still, it is not an issue that could be addressed entirely by organisations alone. There are many factors outside the scope of an organisation that have to be considered. For example, when the focus is on awareness and training for ICT security, then many aspects would be touched upon; such as the overall education system of a country and other structures supporting it. For education and training to ensure sustainable development, it must be responsive to needs of the society, technological progress and globalization trends. Design of training programmes must therefore evolve with time to reflect contemporary demands and has to be based on thorough and proper training needs assessment. Thus it is difficult for an organisation to maintain a sound ICT security culture within its environment while its surrounding environment is not. This is because an organisation interacts with other external parties such as suppliers, customers, and business partners. Hence approaches taken at the national level would tend to be more effective as this would make it possible for achieving a common ICT security culture; this paper has tried to shed some light into this and it is an area that calls for further investigation if the goals stipulated in the OECD guidelines—towards the culture of security are to be realised in practice.

7 REFERENCES

Bakari, J. K., Tarimo, C. N., Yngström, L., and Magnusson, C. (2005) "State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study," icalt, pp. 1007-1011, Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)

Bennell, P., Bendera, S., Kanyenze, G., Kimambo, E., Kiwia, S., Mbiriyakura, T., Mukyanuzi, F., Munetsi, N. Muzulu, J., Parsalaw, W., and Temu, J. (1999) “Vocational Education and Training in Tanzania and Zimbabwe in the Context of Economic Reform” - Education Research Paper No. 28, 122 p.

Bishop, M. (2003) “Computer Security: Art and Science” Addison Wesley Professional: 1st edtn, ISBN: 0201440997.

Chia, P., Maynard, S., and Ruighaver, A.B. (2002b) "Understanding Organisational Security Culture". Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, pages 731-740.

Chia, P., Maynard, S., and Ruighaver, A.B. (2002) “Exploring Organizational Security Culture: Developing a Comprehensive Research model”. IS ONE World Conference, Las Vegas, Nevada USA.

Cohen, Anthony P., (1995) “The Symbolic Construction of Community”. Routledge: New York.

Conolly, P. (2000). "Security Starts from Within." InfoWorld 22(28): 39-40.

Detert, J.R., Schroeder, R.G. and Mauriel, J.J. (2000). A framework for linking culture and improvement initiatives in organizations. The Academy of Management Review, 25(4), 850-863.

DTI (2004) "DTI Information Security Breaches Survey 2004" – Technical report.

Ernst and Young (2004). "Global Information Security Survey".

Freeman, E. (2000). "E-Merging Risks: Operational Issues and Solutions in a Cyber age." Risk Management 47(7): 12-15.

IFIP SEC (2006) - 21st IFIP International Information Security Conference, Karlstad Sweden. (http://www.sec2006.org/ visited last April 23, 2006.

Kowalski, S., (1994) IT Insecurity: A Multi-disciplinary Inquiry, PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm.

Luthans, F., and Kreitner, R. (1984) "Organisational Behaviour modification and Beyond: An Operant and Social learning approach" Glenview, Il: Scott, Foresman.

NHEP (1999) –"Tanzania National Higher Education Policy"

OECD (2002) "Guidelines for the Security of Information Systems and Networks: Towards a culture of Security"

Pfleeger, C. P. (2003) "Security in Computing" 3rd Edn, Pearson Education Inc. Prentice Hall – Upper Saddle River New Jersey 07458; ISBN 0-13-035548-8.

Robbins, Stephen P. (2003) Essentials of organisational behaviour - Prentice Hall, Pearson Education, Inc., Upper Saddle River, New Jersey, 07458.

Rutayuga, A. B., and Kondo, A., (2004) "Reforming Technical and Vocational Education: The Role of NACTE on Assessment and Certification of Technical Education in Tanzania" The 3rd Conference of the Association of Commonwealth Examinations and Accreditation Bodies (ACEAB)- Fiji.

Schlienger, T., and Teufel, S. (2003) "Information Security Culture: From analysis to change" Third annual ISSA - Information Security Conference. Sandton Convention Centre in Johannesburg, South Africa.

Schneier, B. (2000) "Secrets and Lies: Digital Security in a Networked World" Wiley Computer Publishing, ISBN 0-471-25311-1.

Stajkovic, A. D. and Luthans, F. (1997) "A Meta-Analysis of the Effects of Organisational Behaviour modification on Task performance: 1975-95" Academy of Management Journal, pp-1122-49.

Verton, D. (2000). "Companies Aim to Build Security Awareness." Computerworld 34(48): 24.

Wood, C. (2000). "Integrated Approach Includes Information Security." Security 37(2): 43-44.

Yngström, L., (1996) A Systemic- Holistic Approach to Academic Programmes in IT Security, PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm.

PAPER VI

Bridging the Gap Between General Management and Technicians – A Case Study on ICT Security in A Developing Country

Reprinted from

The official Journal of Technical Committee 11 (computer security) of the International Federation of Information Processing (IFIP), The International Source of Innovation for the Information Security and IT Audit Professional, Elsevier, Volume 26, Issue 1, February 2007, pp. 44-55. Also available at URL: http://www.sciencedirect.com

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Bridging the gap between general management and technicians – A case study on ICT security in a developing country☆

*Jabiri Kuwe Bakari**, *Charles N. Tarimo*, *Louise Yngström*, *Christer Magnusson*, *Stewart Kowalski*

Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology, Forum 100, SE-164 40 Kista, Sweden

Keywords:
ICT security management
Organisations
Management
Technicians
Perception problem
ICT-related risks

ABSTRACT

The lack of planning, business re-engineering, and coordination in the whole process of computerisation is the most pronounced problem facing organisations. These problems often lead to a discontinuous link between technology and the business processes. As a result, the introduced technology poses some critical risks for the organisations due, in part, to different perceptions of the management and technical staffs in viewing the ICT security problem. This paper discusses a practical experience on bridging the gap between the general management and ICT technicians.

1. Introduction

The paper outlines a successful mission of how to bridge the gap between general management and ICT technicians. It is based on practical experiences obtained from an ongoing study which aims at developing guidelines for managing ICT security in organisations generally. The study was initially conducted in mid-2004 in five organisations in Tanzania in order to make preliminary observations. Later, at the beginning of 2005, one organisation was earmarked as a test-bed for further observations and here we present some of the findings. The organisation is a government-based service provider operating in 21 out of 26 regions in the country. The organisation has 900 staffs in total and its operations are based on four core services, where three of them are greatly dependent on ICT to meet their intended objectives. The organisation has approximately 2 million customers scattered throughout the country with approximately 25% active customers.

The study was guided by using the Business Requirements on Information Technology Security (BRITS) framework where risks are viewed as part of the actual business rather than primarily as part of the ICT, used together with the Security by Consensus (SBC) model where ICT security is viewed as a social technical problem (Kowalski, 1994; Magnusson, 1999; Bakari, 2005). BRITS is a systemic-holistic framework, combining finance, risk transfer, IT and security in a coherent system. The framework attempts to bridge the gap between top management and IT personnel by translating the financial language into the IT and IT security languages, and vice versa. The translation is achieved by making use of a repository of

☆ The paper was originally presented and published in the Security Culture Workshop at the IFIP SEC2006. This is an updated version.

* *Corresponding author*. Tel.: +46 08 674 72 37; fax: +46 08 703 90 25.
E-mail addresses: si-jba@dsv.su.se (J.K. Bakari), si-cnt@dsv.su.se (C.N. Tarimo), louise@dsv.su.se (L. Yngström), cmagnus@dsv.su.se (C. Magnusson), stewart.kowalski@ericsson.com (S. Kowalski).

0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.10.007

mitigation suggestions, hosted in the Estimated Maximum IT Loss (EMitL) database (Magnusson, 1999; Bakari et al., 2005a,b). In the study the SBC model was used to view and explain security problems as layers of social and technical measures. In addition to these two methods, we also at different stages of the study made use of other methods, namely Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), ITIL (IT Infrastructure Library), Control Objectives for Information and related Technology (COBIT) and the internationally recognised generic information security standard, comprised of a code of practice and a specification for an information security management system (ISO 17799). OCTAVE is a risk-based strategic assessment and planning technique for ICT security (Alberts and Dorofee, 2003). ITIL is a framework for IT management and COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks (ITIL, 2005; ISACA, 2005; ISO 17799).

The findings are organised in a list of 10 initial steps or aspects of importance to successfully bridge the gap. The presentation highlights the motivation and practical experiences of each step.

2. The ten aspects of importance in bridging the gap between the management and technicians

In this section, the 10 steps are introduced and later the experience encountered when executing each step is presented. The steps include:

(i) Getting top management's backing (the chief executive officer (CEO) buying into the idea first)
(ii) Getting technical management backing (the technical department is the custodian of ICT in an organisation)
(iii) Setting up the special ICT security project team (start by forming a provisional ICT security task force)
(iv) Quick scan of the ICT-related risks and their consequences for the organisation (risk exposure due to ICT)
(v) Getting management's attention and backing (the management as a whole need to buy into the idea as well)
(vi) Getting the current status of ICT security documented (take stock of the existing situation)
(vii) Conducting awareness-raising sessions (to allow staffs to recognise ICT security problems and respond accordingly)
(viii) Carrying out risk assessment/analysis
(ix) Working out the mitigation plan (short-term plan for issues that need immediate attention and long-term plan)
(x) Developing countermeasures

2.1. *Step 1: getting top management's backing (the CEO buying into the idea first)*

ICT security appeared to be a new concept to most CEOs in the organisations studied. As confirmed by numerous researches, management backing is important in any effort to improve security in organisations as suggested in some studies (Alberts and Dorofee, 2003; Caralli, 2004; Solms and Solms, 2004; Solms, 2005) and also appears as an important factor in corporate governance as discussed in Control Objectives for Information and Related Technologies (COBIT) by Information Systems Audit and Control Association (ISACA). However, getting an appointment to meet the CEO and talk about ICT security was not easy. In most cases, we were directed to see the IT director or chief security officer. Here one needs to be patient and accept a long-awaited appointment to see the CEO who is always busy and in this case the time slot would be only 10–15 min. Nevertheless, we achieved our goal of meeting them and introduced our agenda on what ICT-related risk is all about and what the challenges are in managing such types of risks. Further, the consequences of not managing such risks for the shareholder value were also discussed, emphasising that today's CEOs will be responsible to their board for the state of ICT security in their organisations. All these were discussed with respect to risk exposure to key performance indicators which may affect the organisation from reaching its mission and business objectives. An example of risk exposure discussed was the problem of business interruption which can be propagated through to the balance sheet with great financial implications and cause embarrassing media coverage, loss of confidence by customers and staffs, resulting in loss of credibility.

2.2. *Step 2: getting technical management backing (technical departments are the custodians of ICT in an organisation)*

It was hard and in most cases almost impossible to talk about ICT-related issues in the organisation without the permission of its IT department. This was mainly due to a perception problem which is also discussed in Bakari et al. (2005a) where the complex problem of ICT security has been relegated to the IT department or rather treated as a technical problem, with no relevant and operational organisation-wide ICT security policy and procedures. Most of those we asked for an appointment gave the following reaction: ''Have you consulted the IT department?'' On the other side, the technical staffs are aware of the ICT security problems, though mostly as a technical concern and not as a business concern. In order to get their support, we had to describe the security problem more holistically, i.e. including both technical and non-technical issues and the reasons why we should include and talk to other departments as well. Our observation indicated that the difference in perception between the management and the technical department made it difficult for the technical department to address the problem adequately. An attempt was made by Bakari et al. (2005b) to address this perception problem using EMitL tool as suggested in the BRITS framework by Magnusson (1999). Getting technical staffs to understand the non-technical components of the problem and how to communicate the problem to the management as risk exposures which needed its attention was yet another important step to take. There were concerns from senior technical staffs on how we were to make the management understand the problem, and what language to use for them to understand.

This was asked by senior staffs, when we were preparing to meet the management team in one of the talks (step 5).

2.3. *Step 3: address the ICT security problem as a special project (forming a provisional ICT security task force)*

> *''Organisations can no longer be effective in managing security from the technical sidelines. Security lives in an organisational and operational context, and thus cannot be managed effectively as a stand-alone discipline. Because security is a business problem, the organisation must activate, coordinate, deploy, and direct many of its existing core competencies to work together to provide effective solutions.''*
>
> (*Caralli, 2004*)

After succeeding in getting the support of the top management and technical management, the important question at this stage was how or where do we start? It was at this stage that we formed the special ICT security project team. The composition of the team included three technical staffs (software, network and hardware), one legal officer, one internal auditor, one security (physical/traditional) officer, and one member of staffs from operational departments (where core services of the organisation are processed). Also one more member of staffs from the insurance department was in the team purposely for risk management as there was no department other than insurance to handle/manage risks in the organisation. All team members were senior members of staffs who have worked with the organisation for more than five years. The main question we faced here was then why to choose staffs from these departments? Our response was based on the facts below and which are also similar to OCTAVE (Alberts and Dorofee, 2003) principles, where the interdisciplinary ICT security project team is staffed by personnel from the organisation itself:

Technical: partly the ICT security problem is a technical issue which could be a result of software, hardware or network problems. In the case of software, there are mostly two fundamental problems, one that affects the application system software and the other that affects the Operating System software. Both could be as a result of the introduction of malicious software (virus, worms, etc.) or system failure, either due to power failure or some other reasons. In the case of hardware, there could be physical damage, a power problem or the hardware or part of it being stolen. Network security can be a combination of both; problems that affect the software and hardware parts of the network. Technical staffs who are working in these sections would be in a good position to give more information about their experience regarding ICT security from a technical point of view.

Auditors: traditionally, auditors are used to audit the financial transactions or operational processes and compliances to laws and regulations, policies, standards and procedures. Given the nature of their work they can also stand back and see the big picture concerning the risk exposure facing an organisation. Auditing ICT is usually considered operational. The one prime focus for ICT audit is security – evaluating whether the confidentiality, integrity and availability of data and services are ensured through the implementation of various controls (ISACA, 2005). It also involves evaluating the realisation of benefits to the business from its investment in IT. Apart from building capacity for internal ICT audit, including the transition from traditional auditing to a hybrid type of auditing (meaning the auditing includes information systems), informed corporate auditors can be in a better position to provide the information needed to advise the management on the importance of paying more attention to ICT security management than technicians' advice.

Legal: as the dependency on ICT in an organisation grows, legal issues such as liabilities, in particular computer/cyber crime (a violation of the law committed with the aid of, or directly involving, a computer or data processing system) are becoming an indispensable part of ICT risk management. Involvement of a legal officer in the team facilitates in addressing the ICT security problems from a legal perspective.

Security: most of the security departments – particularly in the studied organisations – still value physical assets, which means that security strategies end up taking more care of tangible assets than intangible ones. For example, currently CCTVs (close-circuit TVs) are installed in the reception area and along the corridors but not in the server rooms which keep valuable information assets. This situation as revealed here discourages one from stealing tangible company assets from the building as there is a chance of being seen. However, for someone who aspires to steal *information assets*, will have a free ride. By not having the server rooms monitored properly – apart from those who can compromise the assets through the network – it is implied that the security monitoring system is meant for outsiders. Thus, the involvement of physical security staffs helps to identify what needs to be re-engineered for the existing security in the organisation.

Operations: operations is where the core services of the organisation take place. Thus, operations can be an area where the greatest adverse impact on the organisation's mission and business objectives can be observed. In our work we considered having a senior member of staffs from the operations department who is fully knowledgeable of operational transactions. His participation in the team assists in highlighting the operational processes and identifying critical areas of operation. This is an important component in the risk assessment exercise.

Insurance/risk manager: ICT security management is basically risk management focusing on ICT – mainly how to insure valuable assets, including ICT assets.

Human resources: human elements in security tend to be the weakest link in any security chain, even where the best technical security controls are in place (Bishop, 2003). A simple social engineering action, which is a result of not ensuring that staffs are aware of the risks and are familiar with sensible and simple security practices, can ruin the organisation's credibility. Therefore, a strong ICT security management programme cannot be put in place without significant attention being given to human resources. People from the human resources department/unit are responsible for personnel security which, according to ISO 17799, covers not only permanent and temporary staffs of the organisation but also extends to contractors, consultants and other individuals working on the organisation's premises or using the organisation's information and information processing assets.

Furthermore, the human resources department is responsible for recruitment, terms and conditions of employment, including job descriptions and termination. It is also responsible for awareness-raising and training of staffs on security policy, procedures, and techniques, as well as the various management, operational and technical controls necessary and available to secure ICT resources, once such measures are in place (Wilson and Hash, 2003). Inclusion of a human resource person in the team from the beginning helps to take into consideration the human aspects of the security problem from the outset, when designing the ICT security management programme.

Finance: there are two main reasons why finance should be considered. First, all operations of the organisation depend on financial transactions. The roles and responsibilities of staffs vary as compared with other departments due to the nature of their work – financial transactions. Unclear roles and responsibilities can be tolerated in the manual system but not in the computerised financial information system. Secondly, in most cases the end result of any security incident has financial implications; sometimes damage can be propagated to the organisation's final balance sheet.

Selection criteria: generally, the selection was strictly of staffs who have spent a substantial amount of time in the area of consideration and who are also ICT literate, for example, senior auditor with some general computer knowledge. The team was subjected to several orientations about ICT security management in general with reference to the organisation.

2.4. *Step 4: quick scan of the ICT-related risks and their consequences for the organisation (risk exposure due to ICT)*

Before meeting the management as a whole, we needed some kind of justification or evidence of ICT-related risks and their consequences for the organisation. This was obtained by first working out some facts on the likely consequences of ICT-related risks for the organisation. We achieved this by carrying out a quick scan of such risks with the help of the ICT security team. This exercise involved capturing information on what the organisation is doing and how its core services are linked to the use of ICT and hence what kind of risk exposures and their consequences for the organisation. Face-to-face interviews with the CEO, chief financial officer (CFO), IT managers and the heads of the departments involved in the provision of the core services were conducted.

Our interview questions were based on OCTAVE processes 1 and 2, which are primarily for gathering information on the senior management's and operational area management's views of ICT assets, areas of concern, security requirements, current security practices and current organisational vulnerabilities. The two processes are among the four used in OCTAVE phase 1 when building asset-based threat profiles of an organisation as detailed in Alberts and Dorofee (2003, p. 46).

We used the collected information to figure out how the organisation's objectives are supported by ICT assets and in turn what are the possible risks to, and consequences for, the organisation's business objectives as shown in Fig. 1.

We also made use of EMitL tool in an attempt to translate what management sees as damage exposure to corresponding ICT-related risks and hence ICT security properties as shown in Fig. 2.

The tool helped to interpret the technical terminologies of the consequences of losses in the corporate value, based on financial indicators. This interpretation was based on three groups of damage exposure due to ICT risks, namely liability claims, direct loss of property and business or service interruption; also explained in the works by Bakari and co-workers (2005, 2005b). The damage exposures are in turn mapped to ICT security properties.

2.5. *Step 5: getting management's attention and backing (the management as a whole buy into the idea as well)*

The management had to be convinced and understand that their organisation was vulnerable to ICT-related risks. Furthermore, we had to educate them on the magnitude of the security problem, and insist that ICT security was more than technology and more of a human issue. This means it

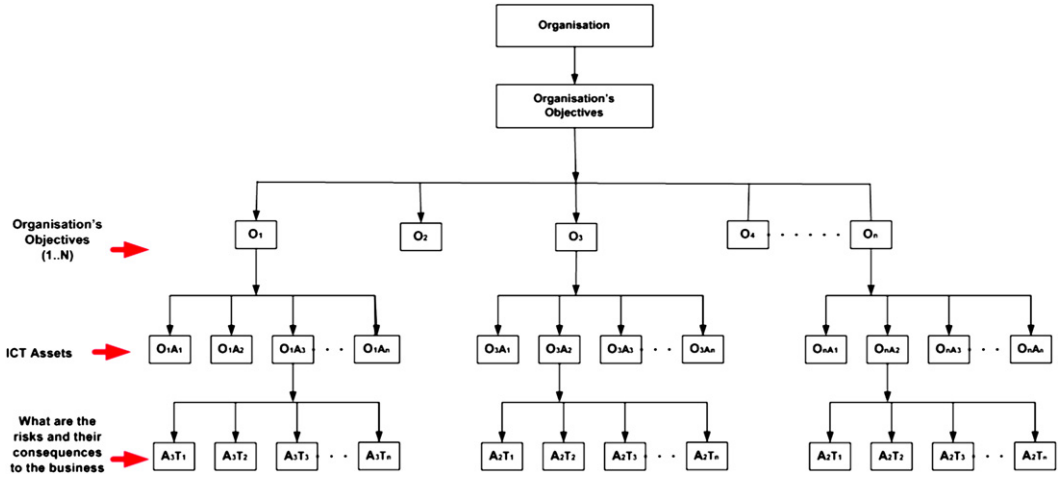


Fig. 1 – Deriving risks to, and consequences for, the organisation's business objectives.

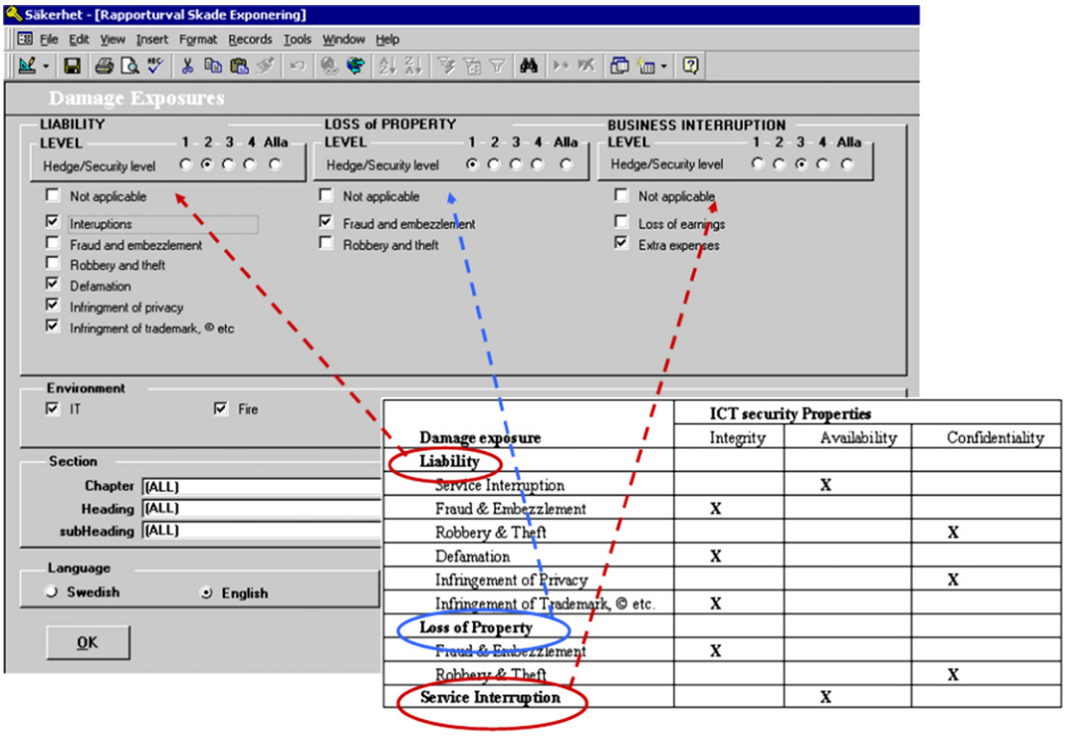


Fig. 2 – Business damage exposure mapped to ICT security properties.

has something to do with the kind of policies and procedures that were in place in the organisation; the type of administration in place, the legal and contractual obligations the organisation had, particularly in delivering services, and also the ethics and culture of the individual staff member. The objective of this step was achieved by presenting to the management the worked-out status of their ICT security obtained in step 4. Diagrammatic representation of the problem and how ICT security was being addressed in their organisation helped to get their attention.

Fig. 3 shows how the problem was perceived on the left-hand side; and on the right-hand side of the figure can be

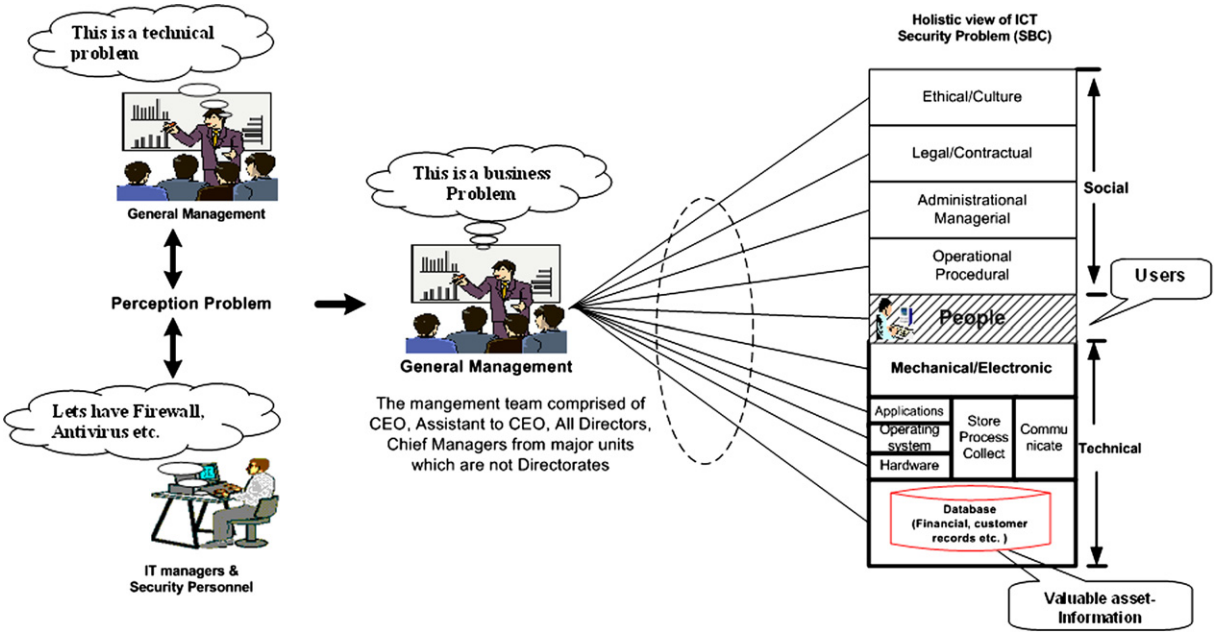


Fig. 3 – How the ICT security problem was perceived and the way it was addressed.

seen a holistic view of the ICT security problem, with people sandwiched between the social and technical aspects, being an extension of SBC model (Kowalski, 1994). For example, we were able to show to the management team, which constituted the CEO, CFO, human resources manager, chief legal officer, chief security officer, chief internal auditor, operational manager, and planning and investment manager, technical managers and other managers, where and how their functions fit into the model. We also highlighted the problem in each dimension and discussed their role in managing the problem with respect to their positions in the organisation.

This was approximately a one-and-a-half hour session with the entire management team. The fact that ICT security management is a multidimensional discipline, as depicted in Fig. 3, was emphasised. We were able to convince the management that this is a business problem, with an ethical/culture dimension, an awareness dimension, a corporate governance dimension, an organisational dimension, a legal dimension, an insurance dimension, a personnel/human dimension, an audit dimension, and finally a technical dimension, also discussed in length in the study by Solms and Solms (2004). It is a socio-technical problem (Kowalski, 1994). We used the figure to demonstrate the management how ICT security is currently being managed in their organisation. The demonstration showed that, currently, the focus is mostly on the technical aspect, meaning that the existing countermeasures are mainly addressing the technical dimension which corresponds to the second and third signs of the 10 deadly sins of information security management as discussed in Solms and Solms (2004). Referring to ISO 17799 and COBIT for the organisational dimension, a management framework should be established to initiate the implementation of information security within the organisation. By using SBC framework, we were able to bring the management team together and discuss the security problem as a business problem as shown in Fig. 3. We were able to point out, with examples, what the security issues in each dimension are and the areas of consideration and consequences if such an issue is not addressed. For example, by highlighting to the management that ''ensuring that staffs/users are aware of information security threats and their consequences for the organisation's mission and business objectives, in the course of their normal work'' was the responsibility of people from the human resources department, helped them to see that this is not a technical department responsibility.

2.6. *Step 6: getting the current status of ICT security documented (take stock of the existing situation)*

Our next step was to have an idea of what existed in the organisation with respect to ICT security. This exercise involved taking stock of what existed in terms of: systems (hardware, software, platforms, networks, applications, users and assets); environment (location and services); security (threat types and potential ones and countermeasures that are currently in place); and procedures (any policies and procedures in place). This information helped to identify the current status of ICT assets, their location and the type of services they provide, as well as threat types for each identified asset and the security measures that are in place. We made use of OCTAVE phase 2, process 5 in some of the stages (Alberts and Dorofee, 2003, p. 49). The OCTAVE phase 2 deals with identification of key components of an organisation's information system. This exercise gave the security team more knowledge of ICT assets, their link to the organisation's objectives and helped to highlight areas that needed immediate attention. In addition, we later used this information during the awareness-raising sessions to help staffs understand and appreciate the types of ICT security problems they have. For example, we established that most of the different types of operating systems currently in use have been un-patched since they were bought; some have security features which are not enabled, and some have no security features at all; the licence status is not clear concerning some of the software; and the existing policy was not helpful as it was outdated and only a few senior staffs knew of its existence.

2.7. *Step 7: conduct awareness-raising sessions among users (with some feedback from steps 1–6)*

At this moment we had gathered information about the organisation, information systems risks and their consequences. We had the full support of the management and the now well-informed internal security team. It was at this step that we rolled out the awareness-raising sessions in the organisation. Our approach was top down as shown in Fig. 4. We

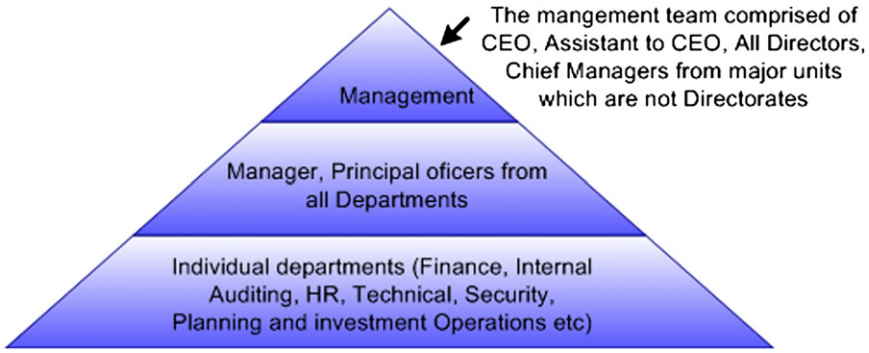


Fig. 4 – Awareness-raising sessions plan.

started with the management and the topic was ''Managing Technology risks, the role of the management, which included legal issues in a computerised environment''.

Along with the presentation notes, we attached the timetable of other training sessions for their departments/staffs as well. This helped to get the message across to other staffs through their bosses who made sure that their staffs attended their respective sessions. The second group was comprised of managers and Principal Officers from all departments. A similar topic was delivered but with a different emphasis from the one used with the management – strategic level. Here the emphasis was mainly on tactical and operational issues. More than 90% of the target groups attended the awareness-raising sessions in person. We made some observations during the sessions. For example, as we looked at the faces of staffs as they were arriving at the awareness-raising session room, we could read their faces saying, ''This session is not for me''. However, after some time into the session the situation changed and people were getting concerned about the issues being discussed. ICT security awareness-raising efforts were designed to allow staffs from various departments to recognise ICT security concerns, participate effectively in the ICT security management process and respond accordingly as suggested in the study by Wilson and Hash (2003), where detailed discussion on 'Building an Information Technology Security Awareness and Training Program' is presented. Apart from the general awareness-raising session, we also had special sessions with individual departments, namely legal, accounts, internal auditing, physical security, human resources and technical. For each session the focus was in accordance with their respective speciality.

For the Legal section, for example, the main point of discussion was what the ICT risks are from the legal perspective and hence the legal issues in a computerised environment. Some questions were posed such as: what are the implications of using unlicensed software in the organisation? How could a crime committed through computers be handled? Are the cooperate lawyers conversant with the subject matter? If not, what are the implications for the organisation should such a problem arise? What we learnt in this particular session, for example, was that participants were very concerned and one of their comments was, ''then we need to revisit our policies and procedures in the computerised environment''.

In the *Accounting* and *Human resources* sections, the focus was on transactions in the computerised environment vis-à-vis roles and responsibilities. We discussed at length the consequences of not having in place a detailed job description, in particular the issue of roles, responsibilities and accountability of staffs when dealing with various transactions such as financial in the computerised environment.

The effect of the awareness-raising sessions was a realisation of the need to go for further training. It triggered staffs, for example, to register for Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) after realising that they needed further training, even if it meant sponsoring themselves. CISA certification focuses on IT auditing, security, and control, while CISM focuses on the information security management (ISACA, 2005). It also triggered the concept of awareness through visiting other organisations (local and international) and preferably in the same industry, to learn what is going on as far as ICT security is concerned. Nevertheless, the local visits only showed that even the other organisations were still at the take-off stage.

2.8. *Step 8: carry out risk assessment and analysis*

Using the security team, we started to conduct risk assessment and analysis starting with the operations department (where core services of the organisation are located), followed by the IT department, physical security and later other departments. The cooperation from staffs was very high due to the effect of the awareness-raising sessions.

As suggested in Magnusson (1999), the need for countermeasures against ICT risks depends entirely on the effect these risks may have on the organisation's mission and business objectives. Fig. 5 is an extension of Fig. 1 and shows how these countermeasures are derived from the organisation's objectives.

(i) Identification of organisation's objectives
In Fig. 5, the objectives are represented by (O_1, O_2, O_3, O_4, …, O_n). The organisation's objectives, which will be taken into account, are those that are ICT dependent.

(ii) Identification of ICT assets that support the organisation's objectives
The second stage involves identification of ICT assets that support the organisation's objective/s (O_xA_x) and the 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 ICT assets. As discussed in Alberts and Dorofee (2003), an 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, an assessment of the threats (A_xT_x) and their consequences that hinder the organisation from meeting its intended objective O_x takes place (where *x* identifies the objective and likewise the corresponding threat, and can be from 1 up to *n* threats). 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 countermeasures for each threat. Picking theft in the previous example, the policy (P_x) may include backup, traceability and recovery, and user policy and procedures.

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 result 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.

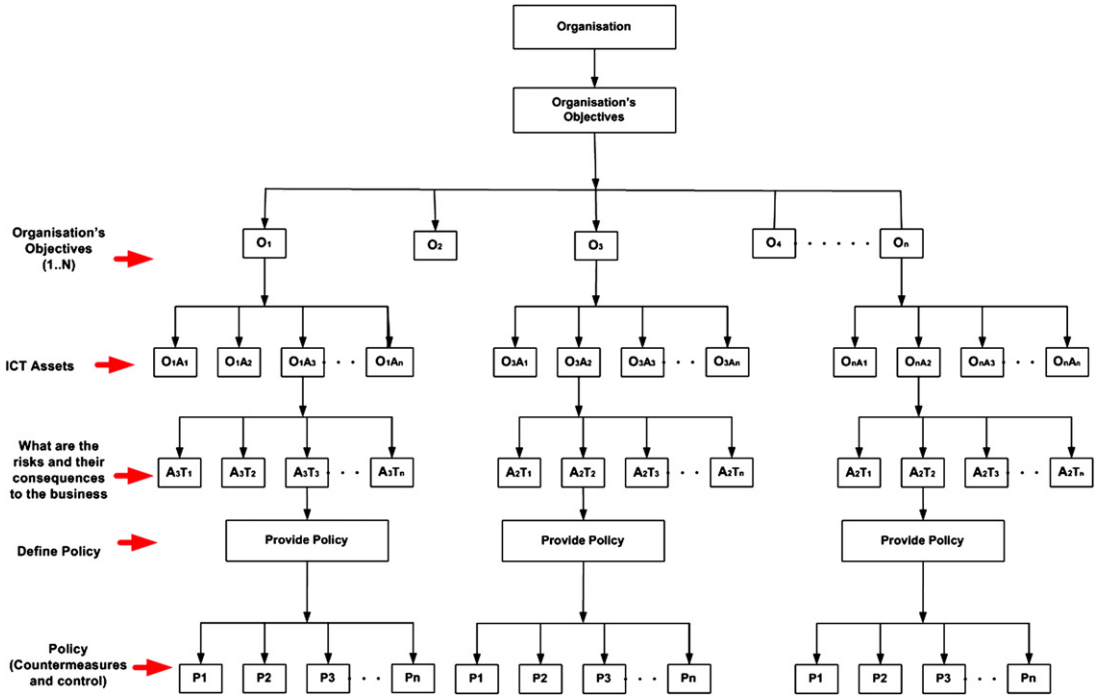


Fig. 5 – Showing how insurance policies can be derived from the organisation's objectives.

This exercise shed even more light on the magnitude of the security problem and information obtained from this step was vital for the discussion we held later with individual managers, in particular when discussing with the CFO on how to financially hedge the identified risks.

In addition, the obtained information was used to estimate security awareness when discussing with the IT department on which countermeasures are being practised and which are not. The discussion also took into consideration the output of the EMitL tool (the output of step 4) (Bakari et al, 2005b).

2.9. *Step 9: work out the mitigation plan (short-term plan for issues that need immediate attention and long-term mitigation plan)*

This is the step that came as a result of pressure from the management. Having realised how risky it was to go without proper ICT security management in place, the management was now at the forefront, suggesting that the security team come up with a mitigation plan. From the management side, an ICT steering committee (management focusing on ICT with security as a priority) was formed where management will work closely with the IT department. The need for control of information technology in use in the organisation was now realised as suggested in COBIT. We made use of OCTAVE method process 8 which involves developing a protection strategy to work out the mitigation plan. From the risk assessment and analysis and the quick scan that took place with the documentation, we found that there were issues that needed immediate attention. They included, for example, getting the issue of licences sorted out, patching the operating systems, training in some areas which were identified as critical but with not enough know-how, and improvement of the infrastructure which was also found to be part of the problem. Although all these were not budgeted for, the management saw the need to reallocate the budget for these immediately as they were seen to be cost effective, having a clear link in safeguarding the organisation's mission and business objectives.

A long-term plan was then worked out which included, among other things, a disaster recovery and business continuity plan, and developing countermeasures which included policies and various mechanisms including procedures on ICT security. These are detailed in step 10.

2.10. *Step 10: develop countermeasures*

The main question here was what set of countermeasures will provide the best protection against the identified risks and the state of ICT security in the organisation. The goal here is to design and develop countermeasures tailored to the organisation that will remedy the identified vulnerabilities and deficiencies. 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 operationalisation stage takes the conceptual level and makes it work in the organisation. This entails, for example, installation and configuration of technical security mechanisms (e.g. user policy and procedures, backup, etc.), as well as information security education and training of employees.

By taking into consideration the suggestion made from the EMitL tool (what should have been in place), ITIL (why), ISO 17799 (what), COBIT (how) and finally the environment in which the organisation is operating, we started deriving the

Policy: *Routine procedures should be established for carrying out the agreed backup copies of data and rehearsing their timely restoration.*

Objective: *To maintain the integrity and availability of information processing and communication services.*

Fig. 6 – Sample policy.

relevant countermeasures to be implemented in order to address the identified ICT risk exposure (ITIL, 2005; ISACA, 2005; ISO 17799). ITIL and COBIT helps in defining objectives of the processes involved in ICT organisation in general where ICT security is a part of the whole. We used ISO 17799 details on what should be done in addressing each dimension. For example, what should be done by human resource people to address the problem associated with ethics/culture. This is detailed under the subsection dealing with personnel security of the standard. Our approach was only to consider those issues that are basic and which can be achieved. This helped us to develop the ICT security policy and corresponding security mechanisms for the organisation. Fig. 6 shows part of the sample policy document where for each policy statement (what) there is the objective (why) which attempts to answer the question why the organisation should have such a policy statement.

For each policy statement we had the corresponding objectives and what type of vulnerability is being addressed. Then there is a pointer to the procedures which show in detail how such a policy is going to be implemented. For example, Fig. 7 shows *how* the above policy and objectives in Fig. 6 were translated into procedures.

This step triggered another concern of redefining job descriptions and responsibilities of the staffs in the organisation. The procedures and security mechanism we developed or suggested then became major inputs in this exercise. In addition, there was a reorganisation of the technical department to include the ICT security function. All these were driven internally through the ICT security project team (formed in step 3). This was achieved in two steps. First reorganisation of the IT department's organisational structure to ensure that there is a clear demarcation of responsibility. For example, system development was separated from the section that deals with change management, and the user department and the interface was centralised at the helpdesk. This was achieved by making use of ITIL (service management process) and ISO 17799 (personnel security). The second exercise

1.1.1 System backup

Full Systems backup shall be done at least once a week or when there is a system change.

1.1.2 Backup Verification

Test restores from backup tapes must be performed once every month. This ensures that both the tapes and the backup procedures work properly.

1.1.3 Storage Period

Available backup tapes must cover a minimum of two weeks. Ideally backups of system data would go back about two months and backups of user data would go back about one month…….

1.1.4 Storage access and security

All backup media must be stored in a secure area that is accessible only to authorised staff. The media should be stored in a special software fireproof safe when they are not in use...

1.1.5 Off-site Storage

Sufficient back tapes so as to provide a full copy of all information for each critical system in the organisation must be stored at a different location ...

Fig. 7 – Sample procedures.

involved brainstorming with the technical department on how the newly developed ICT security policy and procedures could be incorporated into the reviewed sections and the staff's roles and responsibilities. The activities identified in this second step were to wait until the following financial year. In addition, the plans for the new financial budget for each department took into consideration the operationalisation of the proposed countermeasures.

One issue that brought about some discussion was the positioning of the security function in the organisation. Our final conclusion for this, after discussing the advantage and disadvantage of positioning it in different departments, was to have ICT security positioned in the existing security department which was directly under the CEO's office and headed by the chief security officer with overall responsibility for ICT security. Another staff position that was created was that of ICT security administration at the IT directorate level.

Finally, we convened the management team to present the mitigation plan and the proposed countermeasures. One of the key messages that we delivered at the meeting was for them to take responsibility for ensuring that ICT security policy and procedures are approved by the board before full implementation starts. We brought to their attention that it is the responsibility of the board of directors and executive management to provide oversight of the implementation of information security (Posthumus and Solms, 2005), and therefore the outcome of this step (policy and procedures) should be brought to the attention of the board. It was the responsibility of the ICT security project team and IT steering committee to ensure that the policy and procedures come into operation.

3. Discussion

One of the major problems found in organisations today, including our case study, has to do with perception, where the management and general staffs perceive that ICT security is a technical problem and not a business problem. This situation leads to a misunderstanding of the nature of the security problem and consequently ends up in addressing the wrong problem. The observation has indicated that changing the way the management and general staffs perceive the problem is a necessary process and a prerequisite step towards a common understanding of managing ICT security in an organisation. This can be achieved through awareness-raising sessions. Furthermore, the backing and awareness of both management and the general staffs is vital for the success of the ICT security management programme, which leads to the appreciation that the protection of ICT assets is a business issue and not a technical issue.

In the case study, since a sense of security in non-digital (manual) processes exists in the management and staffs in general, what needs to be cultivated is a shift of focus from the manual to the digital process. For example, it is common, in particular in state-owned organisations, to have high security in place on how to handle confidential records in physical registries. This even includes a special type of recruitment of staffs (including vetting), who work in such offices. Being aware, for instance, that system administration is more sensitive than the mere registry, since system administrators have access to more information than that which is already printed, was another milestone. We also found that perception and interpretation of the words ICT security often leads to a misunderstanding of the actual ICT security problem. For example, the traditional interpretation of the word security for many people, in particular in Tanzania (where this study was conducted), meant something to do with physical security, the police, etc., and the word ICT refers to modern technology only. The two key words *ICT* and *Security* should therefore be used carefully. When discussing ICT security with the management, it may sound better if we used Managing technology risks instead of Managing ICT security. Similar suggestions are found in Blakley et al. (2001) where information security is viewed as information risk management. Our experience is that staffs tend to be more cooperative and proactive in dealing with the problem when they understand exactly what ICT- related risks are all about. For instance, sharing passwords or issuing passwords to fellow staff members was not considered such a big deal, because not many staffs realised how dangerous that was.

ICT security is a multidimensional discipline consisting of, among other things, legal, human resources, technical, operations, security, audit, insurance, and finance (Solms and Solms, 2004). It is therefore important that the initialisation process, which involves the formation of a special project team, starts with the right staff. As discussed in the paper, for better results the team must be made up of senior staffs from all major departments (legal, human resources, technical, operations, security, audit, insurance, and finance) to be able to meet the multidimensional requirements of the ICT security problem. Another important aspect is to have practical examples during the awareness-raising sessions coming from the organisation itself, when discussing the ICT-related risks with the management and general staffs. This also helps when discussing the information security plan which must be based on the risk exposure of the organisation itself.

Getting the current status of ICT security of the organisation documented properly gives more knowledge, not only to the security team, but also to the management and general staffs of the interrelationship of ICT assets, threats, and vulnerabilities, as well as the possible impact on the organisation's mission and business objectives. It helps the management and general staffs appreciate the ICT security problem and hence assist in making them more supportive when dealing with the problem. In addition, awareness is very essential to all users but, as discussed before, it will have a significant impact if it is extended and the matter brought to the specific attention of different departments in the organisation. For instance, when meeting corporate lawyers, the main discussion will be on ICT-related risks from a legal point of view.

There are many internationally established codes of practice that are essential in the process of managing information security in an organisation. Studying these multiple sets of practices and guidelines is of importance for determining and understanding the features that are being recommended to organisations and which must be considered when managing information security. In our study, an attempt to approach the problem holistically was used, by initially merging two holistic approaches, BRITS and SBC

model. BRITS gives the business view of the problem and the SBC the security by consensus. The result of the merger was used to approach the problem from the management's perspective as shown in step 5. We have used OCTAVE, ITIL, ISO 17799 and to some extent COBIT, in an attempt to compensate for the missing links in different steps. Looking at these three approaches, ITIL addresses ICT services and operational management practices that contribute to security, COBIT addresses control objectives for information technology security and process control and ISO 17799 is exclusive to the information security management process. A similar study by Solms (2005) has already shown the synergy of combining more than one framework when attempting to manage ICT security in an organisation.

Reviewing the steps as described here, it becomes apparent that they fit well with the issues discussed, such as a framework for information security governance and the like, and those discussed in the 10 deadly sins of information security management (Solms and Solms, 2004; Posthumus and Solms, 2004), although the order in which they appear here might be different.

The process (10 steps) needs to be initiated from outside, but then there is a need to have the process driven internally. Not many organisations have the capability of putting together the ingredients from different methods. An expert is required to interpret and apply different methods and apply what is required in specific stages. Our experience, however, indicated that it is possible to address this problem by extending the proposed holistic approaches into a set of guidelines which can be used to address the problem in the organisation.

4. Conclusion and reflections

Our objective to bridge the gap between the management and the technical department was achieved through the 10 steps. These included: the CEO buying into the idea first; recognising that the technical departments are the custodians of ICT in the organisation; starting it as a special project; showing where the risks and their consequences are; getting the entire management's attention; taking stock of the existing situation; conducting awareness-raising sessions to address the ICT security problem with respect to the organisation's specific environment; carrying out detailed risk assessment; working out a short-term plan for issues that need immediate attention and a long-term plan to finally develop the countermeasures for the identified problems. The study confirmed that the success of the ICT security management process begins with the management realising the importance of ICT security management. That implies that the management allows the organisation, through its own acquired knowledge and confidence, to internalise the practices, thus enabling people to act confidently at all levels. Knowing about the ICT risks and their consequences for the core service operations of the organisation, the management is more likely to offer its support for ICT security endeavours. Likewise, the technical department, following the support from the management, can address the ICT security problem more holistically in collaboration with other departments, by taking into consideration the non-technical dimensions as well.

Discussing bridging of the gap between the management and the technical department in general would also involve other stakeholders as well as looking at other angles of the problem. Within the Tanzanian experience, part of the research into ICT security has covered, in particular, ICT security education and training, ICT security management, Security Controls implementation and ICT systems security assurance (Casmir, 2005; Bakari, 2005; Tarimo, 2003; Chaula, 2003). These are all ongoing activities that hopefully will enable the country to find useful, efficient and socially acceptable ways of balancing the two main perspectives; the social (cultural and structural) and the technical (machines and methods) towards controllable, viable and homeostatic states.

REFERENCES

Alberts C, Dorofee A. Managing information security risks: the OCTAVE approach. Addison Wesley, ISBN 0-321-11886-3; 2003.

Bakari JK. Towards a holistic approach for managing ICT security in developing countries: a case study of Tanzania. Ph.L. thesis, SU-KTH, Stockholm. DSV report Series 05-011; 2005.

Bakari JK, Tarimo CN, Yngström L, Magnusson C. State of ICT security management in the institutions of higher learning in developing countries: Tanzania case study. In: The 5th IEEE ICALT, Kaohsiung, Taiwan; 2005a. p. 1007–11.

Bakari JK, Magnusson C, Tarimo CN, Yngström, L. Ensuring ICT risks using EMitL tool: an empirical study, IFIP TC-11 WG 11.1 & WG 11.5 joint working conference on security management, integrity, and internal control in information systems, December 1–2, Fairfax, Virginia, Washington, US; 2005b. p. 157–73.

Bishop M. Computer security, art and science. Addison Wesley, ISBN 0-201-44099-7; 2003.

Bjorck F. Security Scandinavian style, interpreting the practice of managing information security in organisations. Ph.L. theses, Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, Stockholm; 2001.

Blakley B, McDermott E, Geer D. Information security is information risk management. In: Proceedings of the 2001 workshop on new security paradigms. New York, NY, USA: ACM Press; September 2001.

Casmir R. A dynamic and adaptive information security awareness (DAISA) approach. Ph.D Thesis, SU-KTH, Stockholm; 2005. No. 05-020.

Chaula JA. Security metrics and public key infrastructure interoperability testing. Ph.L Thesis, SU-KTH, Stockholm, DSV report Series 03-021; 2003.

Caralli AR. Managing for enterprise security. USA: Carnegie Mellon University; December 2004.

ISACA. <http://www.isaca.org/cobit/>; 2005 [last accessed on 20 October 2005].

ISO 17799 Standard.

ITIL. <http://www.itil.org.uk/>; 2005 [last accessed on April 2005].

Kowalski S. 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.

Magnusson C. 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.
Solms BV, Solms RV. The 10 deadly sins of information security management. Computers & Security 2004;23(5). ISSN: 0167-4048:371–6.
Solms BV. Information security governance: COBIT or ISO 17799 or both? Computer & Security 2005;24:99–104.
Posthumus S, Solms RV. A framework for the governance of information security (Elsevier Ltd.). Computers & Security 2004;23:638–46.
Posthumus S, Solms RV. A responsibility framework for information security. In: IFIP TC-11 WG 11.1 & WG 11.5 joint working conference on security management, integrity, and internal control in information systems, Fairfax, Virginia, Washington, US; 1–2 December 2005. p 205–21.
Tarimo C.N. Towards a generic framework for implementation and use of intrusion detection systems. Stockholm University/Royal Institute of Technology, Report series No. 2003-022, SU-KTH/DSV/R – 2003–SE; December 2003.
Wilson M, Hash J. Building an information technology security awareness and training program. NIST Special publication 800-50; October 2003.

Jabiri Kuwe Bakari is a Ph.D. student studying potential solutions in relation to the management of ICT security (holistic approach), at the Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology in Sweden. He received his B.Sc. Computer Science degree at the University of Dar-es-Salaam Tanzania in 1996, M.Sc. (Eng.) Data Communication degree from the Department of Electronic and Electrical Engineering, Sheffield University in UK in 1999, and Licentiate of Philosophy degree from the Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology in Sweden in 2005. He is an active member of the International Federation for Information Processing (IFIP) TC-11 Working Group 11.1, and IEEE. He has published and presented several papers in the field of information security management at the ISSA, IFIP, IEEE and IST international conferences.

Charles Tarimo is currently a doctoral candidate in computer and communication security at Stockholm University, Department of Computer and Systems Sciences. He holds a B.Sc. in Engineering (B.Sc Eng.) obtained in 1994 from the University of Dar-es-Salaam, Tanzania and a Licentiate of Philosophy (Ph. lic.) in Computer and Systems Sciences, obtained in 2003 from Stockholm University in Sweden. Charles is an employee of the University of Dar-es-Salaam Tanzania. His research interests are focused on operational and practical issues with regard to aspects of requirement development, designing, implementation, and maintenance of different technical and non-technical ICT security controls within organisations, such as Intrusion Detection Systems.

Louise Yngström is a Professor at the Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology. She is also the Director of SecLab, Dean of research studies, and responsible for national and international masters programmes in ICT security. She started one of the very first interdisciplinary academic IT security programmes in the world in 1985, naming it ''Security Informatics''. She was awarded her Ph.D. in 1996 for the introduction of a methodology for such academic programmes, called the ''Systemic-Holistic Approach'' (SHA), where ''soft'' and ''hard'' sciences appropriate for IT security issues are mixed. Being one of the pioneers in the field of systems sciences and security in Sweden, she has been with the department since 1968. Dr. Yngström founded IFIP's WG11.8 and the World Conference on Information Security and Education, and is an active member of various working groups within IFIP TC9 (Social accountability of IC&T) and TC-11 (Computer Security).

Christer Magnusson is an Assistant Professor at the Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, specialising in IS/IT Security and IS/IT Risk Management. He brings two decades of industrial and academic information security experience to our group. Before joining SecLab, Dr. Magnusson was the Head of Corporate Security and Risk Management at Sweden Post and CEO of Sweden Post Insurance AB, and he has also been the Head of Corporate Security in the Ericsson group. He has also worked within the IT Security group of the Swedish Agency for Public Management (Statskontoret). Dr. Magnusson was awarded the SIG Security Award by the Swedish Computer Society in 1999 and in 2000 the Security Award by the Confederation of Swedish Enterprise (Svenskt Näringsliv) in recognition of the models and the integrated processes regarding IS/IT Risk Management that he developed as a part of his research studies. He holds M.Sc. and Ph.D. degrees in Computer and Systems Sciences.

Dr. Stewart Kowalski is a part-time lecturer and advisor at the Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology in Sweden. He has over 25 years experience in teaching and IS/IT security. He is currently the Risk Manager for Ericsson Global Services which operates in over 140 countries around the world. His research interests include industrial and academic research in the development adoption and assimilations of IT security technologies and practices in organisations, markets and cultures.

PAPER VII

Operationalisation of ICT Security Policy, Services and Mechanisms in an organisation.

Reprinted from

The Proceedings of the IST-Africa 2007 International Conference
to be held at Joaquim Chissano International Conference Centre,
Maputo, Mozambique
09 – 11 May 2007. (Forthcoming)

Operationalisation of ICT Security Policy, Services and Mechanisms in an Organisation

Jabiri Kuwe BAKARI[1], Christer MAGNUSSON[2], Louise YNGSTRÖM[3], Charles TARIMO[4]
Stockholm University, Forum 100, Stockholm, SE-164 40 Kista, Sweden
Tel: +46-8-16 1697, Fax: + 46-8-703 90 25,
Email: si-jba@dsv.su.se[1], cmagnus@dsv.su.se[2], louise@dsv.su.se[3], si-cnt@ dsv.su.se[4]

Abstract: The problem of ICT security is of concern to many ICT-dependent organisations, despite the many security control solutions available. For some organisations it is due to a complete lack of an ICT security policy. Even where a policy exists, problems can arise due to problems of interpretation to appropriate security services, mechanisms and their operationalisation. In some places the policy exists but not approved by the board, and in other places, although approved by the board, it ends up on the shelf; yet in others, apart from the senior staff, nobody else knows even of its existence. Where implementation of ICT security policy, services and mechanisms exists, it is done on an ad-hoc basis, thus ICT security problems continue. In the case presented here, lack or inadequate operationalisation of ICT security policy, services and mechanisms was found to be one of the major challenges. Thus, this paper outlines practical experience on how ICT security policy, services and mechanisms can be operationalised in an organisation.

Keywords: ICT Security Management, Policy, Services, Mechanisms, Operationalisation

1. Introduction

The ICT security problem encompasses any deliberate act affecting three fundamental properties of an information system. These properties include confidentiality, integrity, and availability. ICT risks can affect individual users, small and large organisations and governmental services, and have financial implications too, for example, direct costs, such as the theft of money, digital assets, or sensitive information. It can also cause indirect costs in the form of service interruption, legal liability, and lower productivity due to diverted resources such as bandwidth and computing power, all of which have negative effects on meeting the organisation's objectives with financial implications [1, 2].

In earlier studies [3, 9] dealing with the state of ICT security management in developing countries, the findings indicated: lack of awareness of how vulnerable the studied organisations are; too much dependence on the ICT vendors or suppliers; lack of regular and reliable back-ups for sensitive systems and information; lack of personnel who are responsible for ICT security; lack of clearly defined roles and responsibilities for personnel; perception that the ICT security problem is a technical one and therefore relegated to the IT department with no support from the management and other departments; and the belief that top-of-the range firewall and anti-virus will solve the security problem.

From these earlier studies [3, 9], organisation "Y" (Size: 900 staff and branches throughout the country—Tanzania - where these studies were conducted) was identified for further study as a test-bed for the following reasons: the organisation was in the process of migrating from proprietary systems to open, inter-operable platforms with TCP/IP as the foundation. In the process of migration, the organisation was planning to implement 9 information systems which involved migration from a closed ICT environment (operating

in a sort of island – where all data were collected from different branches/regions and processed centrally) to a new, open, inter-operable system, together with the organisation's mission to have the services available through the internet.

This increased the organisation's exposure to ICT security vulnerabilities. In particular these were the major problems found: a) the existing ICT security policy was outdated, not enforced and lacked interpretation to appropriate security services and mechanisms, hence the few existing security mechanisms were only on an ad-hoc basis; b) lack of clearly defined ICT security responsibilities as such nobody was accountable in case of a problem; c) poor documentation, classification and control of ICT assets (hardware, software, information), d) lack of business continuity plans; and e) lack of procedures on how to handle ICT assets. Hence there was an immediate need to improve the management of ICT security in the organisation to control the ICT security problems.

In the course of our study in organisation "Y", we were able to establish that one of the major causes of these problems was the inadequate operationalisation of an ICT security policy, services and mechanisms in the ICT security management process in that the policy was there and ICT security control mechanisms were installed/implemented but there was no correlations between the implemented controls/mechanisms and the contents of the policy. In other words the decision to implement a particular ICT security control was not always based on what is in the policy but rather on the apparent need for it.

This paper captures the practical experience we encountered in operationalising the ICT security policy, services and mechanisms in this organisation. According to Bishop [1], "a security policy is a statement of what is, and what is not, allowed" and "a security mechanism is a method, tool, or procedure for enforcing a security policy". The security services are logical services – specified independently the physical mechanism used to deliver them [17]. The goal of the ICT security policy, services and mechanisms is to define the organisation's expectations of proper use of information systems and to define services and mechanisms to prevent, detect and respond to ICT security incidents [15].

Section 2 outlines the method and position of the study with respect to other related studies. The operationalisation of the ICT security policy, services and mechanisms is detailed in section 3, followed by the conclusion in section 4.

2. Methodology

Figure 1 gives a complete overview of the ICT security management process (steps) we have developed through a number of action-research oriented studies [3, 4, 9]. However, in this paper the focus is on activities involved in step (GL-11) given the problems explained earlier. The other parts of the guidelines can be found in [4].

In the figure, examples of the problems we cited in the introduction, such as lack of business continuity plans, are all reflected in the risk assessment (GL-08) and in turn the plans, policies, services and mechanisms required to mitigate each of them are worked out in steps (GL-09) and (GL-10). Then the two steps (GL-09) and (GL-10) becomes major inputs to (GL-11)—Operationalisation of ICT security policy, services and mechanisms.

In the study, the overall introduction of the security management process, as depicted in figure 1, involved senior staff who have been working with the organisation for a long time and had enough experience in their working area from each major department. Apart from the risk assessment outputs, ISO 17799, Control Objectives for Information and related Technology (COBIT) and IT Infrastructure Library (ITIL) were also consulted for the accomplishment of (GL-09) and (GL-10) [4, 5, 6, 7].

For each step in the security management process, a categorisation is used as proposed by Kowalski [12], taking into account the social and technical dimensions sandwiching users, as shown in figure 2. These categorisations include: ethical/culture; legal; administrative and managerial; operational procedures; policy and technical issues.

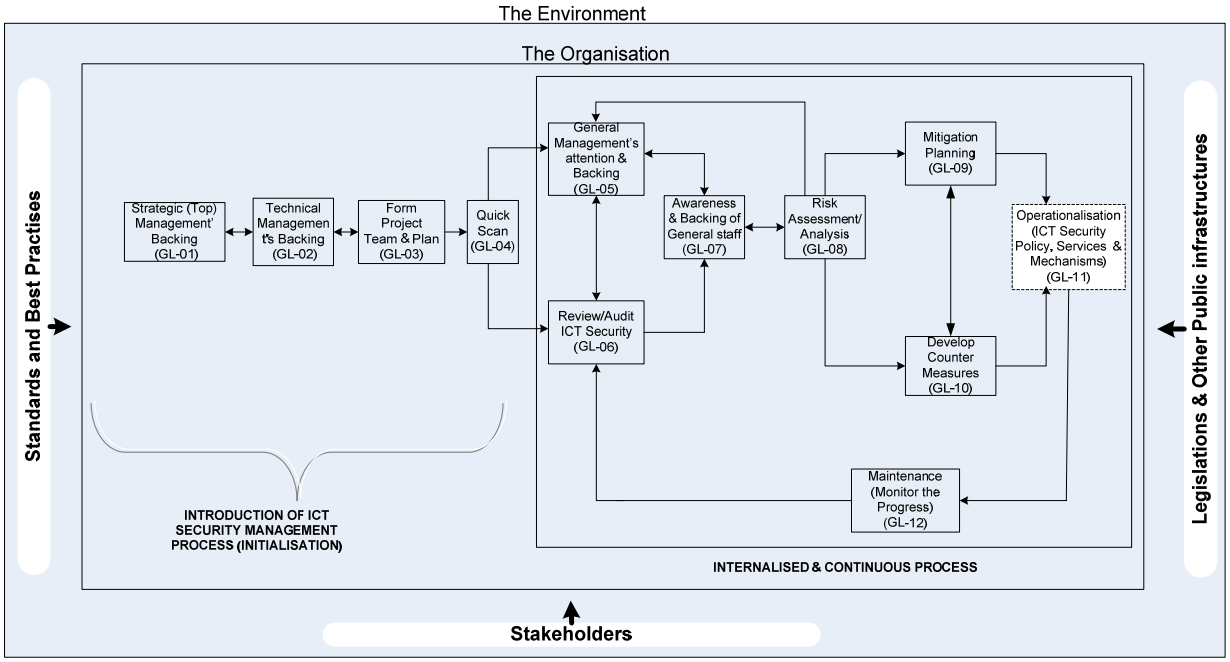


Figure 1: ICT Security Management Process

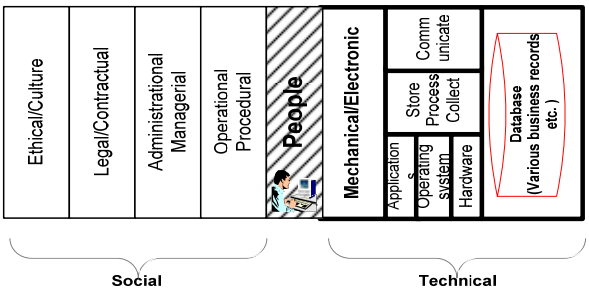


Figure 2: Holistic View of ICT Security Problem

Hence the findings from the study [3, 4, 9] and the experience of the intervention in organisation Y are used here as input to underline how the ICT security policy, services and mechanism plans can be successfully put into operation in the organisation. With reference to figure 1, this paper focuses on the operationalisation of ICT security policy, services and mechanisms as depicted in the highlighted box.

3. ICT Security Policy, Services and mechanisms Operationalisation

Operationalisation (ICT Security Policy,Services & Mechanisms) (GL-11)

A major outcome of the ICT risk assessment and analysis is the mitigation planning which includes the countermeasures proposal for the identified ICT security problems. The outcome of the risk assessment also helped us to update the ICT security policy, services and mechanisms for the studied organisation. In principle, for each identified problem, a policy statement was proposed. For each policy statement (what), you have the objective (why), which attempts to answer the question as to why the organisation should have such a security policy statement in the policy document. ICT security policy alone will not suffice without security services and corresponding mechanisms on how the proposed policy should be effected. ICT security policies are qualitative—statement of intent; they do not say exactly or specifically how the proposed policies can be achieved. It is therefore important that service such as intrusion detection and mechanisms such as intrusion detection systems are more explicit and, where possible, explained quantitatively, so that the policy is easy to implement, enforce, measure and audit [1, 15]. In figure 3, we show how corporate policy is mapped with security services, mechanisms and resources.

For each security service *S*, there must be at least one mechanism *M* to support it, which in turn may have sub-mechanisms that must also be assigned to resource *R* in a particular department. The resource can be allocated to a technical or non-technical department. A mechanism can be a procedure and tools (e.g. ant-virus or hardening of operating system security) to be used and the resource can be a member of staff.

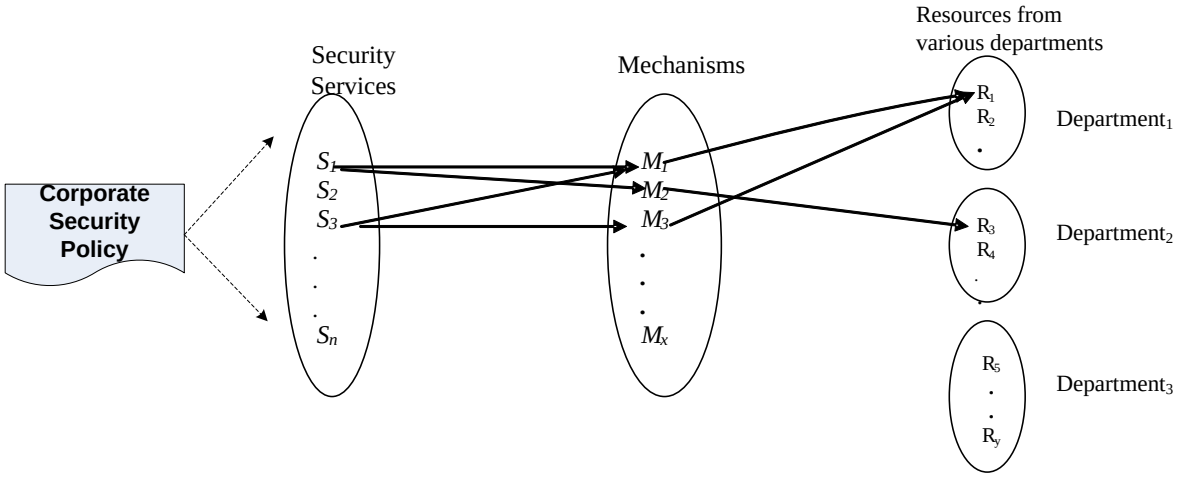


Figure 3: Mapping Policy, Services, Mechanisms and Resources

For example, if one proposes a policy statement which will result in a security service such as data replication and backup, the corresponding mechanism must relate to the actual backup of for instance particular business records. This must be followed by routine procedures showing the type of data or systems (whether critical or not), frequency of backups, whether on- or off-site, and what resources are required. These procedures should be reflected in the roles and responsibilities of a particular department and consequently reflected in somebody's job description. Now since we know the type of data, volume and sensitivity, we can then have a clear indication of what type of backup facilities should be in place. In addition, one must make sure that the staff responsible for this backup process actually know how to go about the process. Figure 4 shows how ICT security policy is being translated to various or corresponding ICT security, services and mechanisms.

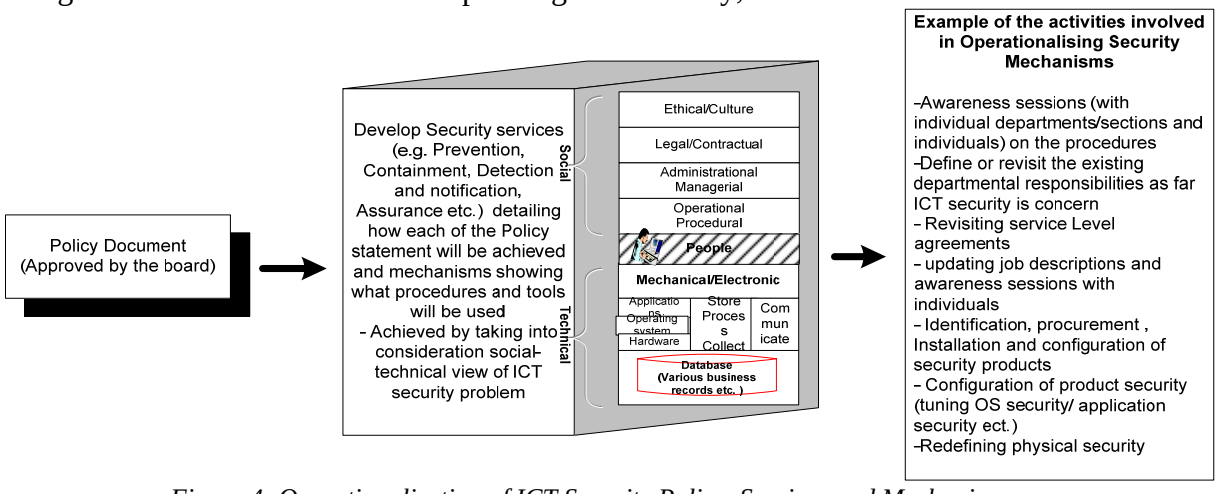


Figure 4: Operationalisation of ICT Security Policy, Services and Mechanisms

It is a common mistake to believe that after development of the ICT security policy, services and mechanisms, the implementation can be left to the technical department. This can only solve one part of the problem—the technical one shown in figure 2, putting in place tools such as firewalls, IDS, ant-viruses, proper patching management [12], but leaves out the procedural and human aspects. Indeed, the technical department has its role to play. However this should take place together with other departments in accordance with the

holistic approach (social-technical as shown in figure 2) of addressing ICT security problems (interdisciplinary). The following sections underline a few examples of the roles, responsibilities and reorientation of departments in an organisation, when it comes to implementation of ICT security policy, services and mechanisms, based on observations in the main study [9] and in particular our experience in organisation (Y)—the test-bed.

3.1 - Executive Management (from the Technical Department to the Board Room)

Our presentations of risk analysis findings and the proposed mitigation plans to the management, triggered the re-establishment of an ICT steering committee, chaired by the Chief Executive Officer (CEO) [Used in this study to mean people in the top senior position], for guiding and overseeing the implementation of the recommendations. We were able to convince the executive management that they are responsible for overseeing the development of the policy, recommending the ICT security policy to the board for approval and thereafter they are responsible for the management and implementation of the policy as suggested in [5, 6]. Another important factor was the backing we got from the general management and the general staff as a result of awareness sessions. As such, the preparation of the policy, services and mechanisms as suggested in [4] was internally driven. This resulted into formation of a team led by the corporate lawyers and consisting of senior staff from the technical, human resources, internal auditing, security, operation and planning departments. This team was then responsible for assisting the executive management through the ICT steering committee in taking the policy document to the board for approval. The exercise involved among other things the amendment of the existing staff regulation to include ICT security-related penalties etc.

3.2 - Internal Audit Department

Among the findings in our study, was the presence of ACL (Audit Command Language) auditing software which was rarely used. Through the individual departmental awareness sessions with the audit department it triggered re-training on the use of the software and checking its licence status. Also as supported by Salman [8], apart from building capacity for internal ICT auditing and the changes from traditional auditing to a hybrid type of auditing, which includes information systems, we found that informed corporate auditors can be in a better position to provide the needed information to advise the management on the importance of paying more attention to ICT security management. Here it was recommended that the Audit department be reorganised to include an Information systems security auditing function in order to oversee all ICT auditing functions.

3.3 - Security Department

In organisation “Y” the focus of the security department has been to take more care of tangible assets than the intangible ones. For example, CCTV (closed-circuit TV) was installed in the reception area and even along the corridors, but not in the server rooms which keep a valuable asset—information. We also learned that part of the physical security services was outsourced. As overseer of Security in the organisation, it was recommended that the department be reorganised to accommodate ICT security.

3.4 - Information Technology Department

In organisation “Y”, the IT department has responsibility for the planning, development, implementation, management, control and maintenance of ICT in accordance with the established ICT policy and strategies of the organisation. In order to accommodate the new role of managing ICT security, the IT department had to reorganise themselves to reflect the new demands and requirements of ICT security, as well as conducting staff re-orientation. In the course of our study, a section responsible for ICT security was established to oversee ICT security mechanism implementation based on the policy. In

order to achieve this work, job descriptions were redefined to reflect the new role of ICT security. The job description defines staff roles and accountability. Without job descriptions it is not possible for staff to be properly committed to, or be held accountable for, a role.

3.5 - Human Resources Department

The operationalisation process involves people—staff. Our findings indicated that involvement of the human resources department from the beginning in the entire ICT security management process is very vital, since they are in principle the owner of "human resources" in the organisation. It is true that technical security controls for ICT systems are critically important, but it is equally important to take a note that they largely depend on the people who operate and come into contact with the systems in their daily duties [1, 10, 13]. We realised, for example, that all efforts can turn out to be useless by simple social engineering and the like, which is a result of not ensuring that staff are aware of the risks and are familiar with sensible and simple security practice. Awareness sessions which also resulted in specialised training in some cases were crucial in that they made staff understand the link between the proposed ICT security measures and their implication for the organisational goals. What was important to stress when we were working with human resource department was the link between awareness/training and the staff's roles and responsibilities when it comes to operationalising ICT security policy, services and mechanisms. For example, auditors responsible for auditing and reporting on compliance with the ICT security policy and standards should attend special training sessions in that area. The same applies to corporate lawyers, IT technical staff and other departments at different levels (strategic, tactical and operational).

3.6 - Legal Department

The first thing that we discussed with legal people was to let them know that any ICT security breach will need legal interpretation. Through examples, we helped them to understand that, as ICT dependence in an organisation grows, legal issues, in particular in relation to computer/cyber crime (a violation of the law committed with the aid of, or directly involving a computer or data processing system) are becoming an indispensable part of ICT security management. We found out that all policies, regulations, contracts and agreements should go through their department at some stage. One of the immediate reactions we got from the legal people during the individual department awareness session with them was ".. We need to review most of our policies, staff regulations and even some of our contracts .." The lesson learned here is that where corporate lawyers exist, they should be well informed and prepared to address such problems, through specialised training or awareness sessions and in liaison with other organisations on how to handle ICT-related problems in line with the prevailing legal framework of the country.

3.7 - Operations Department

In the studied organisation, the Operations department is the main source of risk exposure and preventing the organisation from achieving its mission and business objectives. This is where most of the data are collected, entered and transacted throughout the organisation's information systems. According to Bishop [1], the source of information gives credibility to its accuracy, causing the user to place their trust on the information. Any data integrity problem introduced here can be propagated throughout the whole system. The studied organisation was in the transition, migration from a closed ICT environment (operating in a sort of island – where all data were collected from different branches/regions and processed centrally) to a new, open, inter-operable system. This means data has been collected in the branches and sent to the head office through some kind of media. This is an even more

vulnerable situation which can again be addressed through well planned staff awareness and training to handle their duties and comply with the ICT security policy and procedures.

3.8 - Other Departments

In general, we found that all departments have to be reorganised to assume the new role of ICT security services and mechanism operationalisation. This involves redefining the roles and responsibilities of each department and the job descriptions and orientation of all staff.

3.9 - More Specialised Training

The effect of the awareness-raising sessions was a realisation of the need to go for further training. It triggered, for example, more staff from Accounts, audit and technical sections to register for Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) after realising that they needed further training, even if it meant sponsoring themselves. CISA certification focuses on IT auditing, security, and control, while CISM focuses on information security management [14]. In addition, the legal department was able to source tailor-made training for ICT and the law, while people from the security department were more into forensic training.

3.10 - Positioning Main ICT Security Function

One of the challenges we faced during the study was the process of determining where to position the ICT security function in the organisation. The first obvious placement was under the IT department. The advantage of this option was that the IT director understands the nature of the information systems in the organisation, and therefore good support would be expected from him. The downside of this option was that, for the IT director, IT security problems are seen as part of other IT problems, which means it may not receive the attention it deserves. This was observed even during this study. But most important is that even the IT directorate needs to be checked for compliances as a whole.

The second alternative was to place it under the security department. In the studied organisation, the security department was found to mainly focus on traditional security (mainly physical security). In that case the focus is on physical security, and so it could help, for example, with incident investigations. However, there was a significant cultural difference between information security and physical security functions. The chief security officer, although appreciating our efforts, lacked ICT security knowledge, and so may be a poor communicator with the CEO on matters related to information security as also observed by Budnik in [11]. The Internal Auditing department was another possible candidate. The advantage of this is that auditors are well informed of the risk to the entire organisation. However, it was not recommended due to the conflict of interest that would arise as a consequence of the Internal Audit mandate to review the work done by other units, including the Information Security Department and that the department itself needed to be re-engineered to be able to carry out its primary duties in the new ICT environment.

The last example was that of attempting to include it in the overall risk management process within an organisation. The drawback was that the studied organisation did not have a risk manager, only an insurance manager who was not familiar with technology.

Our analysis indicated that positioning the ICT security function under a department which is at least one layer from the CEO may result in poor control and effectiveness when enforcing organisational ICT security. The question was can we form another department? Probably it is a matter of change of culture in the organisation where the current security department (traditional) incorporates the ICT security function. Depending on the nature of the organisation and business, the answer to this question may vary. Our suggestion was to incorporate ICT security function in the current security department, since they report directly to the CEO and suggested to improve their capacity in ICT security.

4. Conclusion

Our objective to operationalise an ICT security policy, services and mechanisms in the studied organisation was achieved through a number of steps. These included mapping corporate policy to relevant security services, mechanisms and resources; awareness sessions for the general management and for general staff; establishment of an ICT steering committee to oversee the operationalisation process; redefine and revisit departmental responsibilities including individual job descriptions; provide specialised training; restructure some departments; and clearly define and place the overall ownership and authority of the ICT security function in the organisation. The operationalisation of the ICT security policy, services and mechanisms becomes an internalised and continuous process which will support the entire organisation in present and future endeavours.

The overall ICT security management process is challenging for many organisations. We have shown how operationalisation of an ICT policy, services and mechanisms has been achieved in an organisation in a least developed country environment [16], characterised as low-income countries suffering from long-term constraints against growth. Growth constraints include low human resource development, and severe structural weaknesses in the economic, social, and political realms. Awareness and backing of senior management, general management and staff was essential to make this process work as well as defining the true overall ownership of the ICT security function within the organisation.

References

[1] M. Bishop, “Computer Security, Art and Science”, Addison Wesley, USA, 2003.

[2] OECD (2006) OECD Studies in Risk Management, Norway INFORMATION SECURITY ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. Web site, URL: http://www.oecd.org/dataoecd/36/16/36100106.pdf. (Accessed on 21st November, 2006)

[3] J. K. Bakari, C. N. Tarimo, L. Yngström & C. Magnusson, ”State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case study”. IEEE Advanced Learning Technologies”, Kaohsiung, Taiwan July 5 - 8, 2005, pp. 1007-1011

[4] J. K. Bakari, C. N. Tarimo, L. Yngström, C. Magnusson, & S. Kowalski“Bridging the gap between general management and technicians – a case study in ICT security in a developing country” Journal of Computer & Security,2007 , Volume 26/1, pp. 44 – 55.

[5] ISO 17799.

[6] B. V. Solms “Information Security governance: COBIT or ISO 17799 or both?” Journal of Computer & Security, 2005 Volume 24 pp. 99-104.

[7] http://www.itil.org.uk/ Last accessed on April, 2005.

[8] S. Salman “Knowing Your Audience: IT Auditing in Developing Countries”, August, 2005, Available at http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=5638, accessed on 12th August, 2006)

[9] J. K. Bakari, “Towards A Holistic Approach for Managing ICT Security in Developing Countries: A Case Study Of Tanzania”, Ph.L thesis, Report Series No. 05-011. Stockholm University. (2005).

[10] M. Wilson & J. Hash “Building an Information Technology Security Awareness and Training Program”, NIST Special Publication 800-50, 2003.

[11] K. Budnik, “Managing Information Security, a practical approach” ISSA 2006, Johannesburg, South Africa, Deloitte Security Services Group.

[12] S. Kowalski “IT Insecurity: A Multi-disciplinary Inquiry”, Ph.D Thesis, Report Series No. 94-004. Department of Computer and Systems Sciences, Stockholm University, 1994.

[13] C. P. Pfleeger, C. P. “Security in Computing” 3rd Edn, Pearson Education Inc. Prentice Hall – Upper Saddle River New Jersey, 2003.

[14] ISACA, 2005. http://www.isaca.org/cobit/ (Accessed on 20th October, 2005

[15] T. R. Peltier, “Information Security Policies, Procedures, and Standards, Guidelines for Effective Information Security Management”, AUERBACH, 2002

[16] K. M. Gelan, “A Theoretical Model for Telemedicine: Social and Value Outcomes in Sub-Sahara Africa”. Ph.D Thesis. Report Series No. 06-020. Department of Computer and Systems Science, Stockholm University, 2006.

[17] J. Sherwood, A. Clark and D. Lynas “Enterprise Security Architecture, A Business-Driven Approach” Computer Security Institute CMP Books, San Francisco, 2005

Part III

Appendences

Appendix A-1

Appendix A-1 – Introduction letter to the Organisation

UNIVERSITY OF DAR ES SALAAM
OFFICE OF THE VICE-CHANCELLOR
P.O. BOX 35091 • DAR ES SALAAM • TANZANIA

Ref. No: AB3/12(B)
Date: 9th August, 2004
To: The Director General,
Name of the organisation
Dar es Salaam.

UNIVERSITY STAFF AND STUDENTS RESEARCH CLEARANCE

The purpose of this letter is to introduce to you **Mr. Jabiri K. Bakari** who is a bonafide student of the University of Dar es Salaam and who is at the moment conducting research. Our staff members and students undertake research activities every year especially during the long vacation.

In accordance with a government circular letter Ref.No.MPEC/R/10/1 dated 4th July, 1980 the Vice-Chancellor was empowered to issue research clearances to the staff and students of the University of Dar es Salaam on behalf of the government and the Tanzania Commission for Science and Technology, a successor organization to UTAFITI.

I therefore request you to grant the above-mentioned member of our University community any help that may facilitate him to achieve research objectives. What is required is your permission for him to see and talk to the leaders and members of your institutions in connection with his research.

The title of the research in question is **"Managing ICT Security in organisations in the developing world: A case of Tanzania."**

The period for which this permission has been granted is from **16th August 2004** to **15th August, 2005** and will cover the following areas/offices: Name of the Organisation.

Should some of these areas/offices be restricted, you are requested to kindly advise him as to which alternative areas/offices could be visited. In case you may require further information, please contact the Directorate of Research and Publications, Tel. 2410500-8 Ext. 2087 or 2410743.

/Prof. M.L. Luhanga
VICE-CHANCELLOR

UNIVERSITY OF DAR ES SALAAM
P. O. BOX 35091
DAR ES SALAAM

Direct: + 255 22 2410700/2113654
Telephone: + 255 22 2410500-8 Ext.2001
Telefax: + 255 22 2410078/2410514
Telegraphic Address: UNIVERSITY DAR ES SALAAM
E-Mail: vc@admin.udsm.ac.tz
Website address: www.udsm.ac.tz

Appendix A-2

Appendix A-2 – Introduction letter to respondents

Dear Sir/Madam,

I would like to utilise your experience as …… in those matters related to ICT security at the Organisation **X**.

I am carrying out research at the department of Computer and System Sciences, Stockholm University/Royal Institute of Technology in collaboration with the University of Dar-es-Salaam, focusing on potential solutions in relation to the management of Information and Communication Technology (ICT) security in developing countries. As part of that research, organisation **X** has been earmarked as one of the five organisations in Tanzania to be used as a case study.

Please spend a few minutes going through the introduction section to get an overview and objective of this survey questionnaire.

Information presented in this questionnaire will only be used for the purpose of this survey. In the description of results of this survey no identification of individual persons will be made. Individual answers will be kept confidential, i.e. the answers will be analysed, consolidated and presented by category of staff and organisations.

Thank you in advance for your valuable time and consideration.

Regards,

J. K. Bakari
Ph.D. Student
Mobile phone: 0744-766762 Dar es-Salaam
E-mail: si-jba@dsv.su.se

SURVEY QUESTIONAIRE

1.0 Introduction

The use of ICT in developed countries has changed economies and the way businesses are run. The use and development of ICT capabilities, however, faces a wide range of constraints and challenges in the developing countries.

Every day new types of ICT products and services are finding their way into our offices, schools and homes affecting the way we learn and live. The consequences of this ICT revolution for society are almost impossible to enumerate. The ability of an organisation to achieve its mission and meet its business objectives is directly linked to the state of its information systems, whose assets are intangible in nature. Systems store, process, and transmit the critical information that drives an organisation's business.

ICT-dependent organisations must have financial protection against ICT risks. The reason for this is that the organisations' goals will most likely be more affected by financial consequences of ICT risks than by traditional risks as, for instance, fire.

Currently the focus of both commercial and non-commercial organisations in developing countries like Tanzania is on what is commonly known as "Computerisation". Very little or no attention at all is paid to the procedures on how to use ICT. More serious is the security of critical information systems, and consequently their effect on the organisation's mission. Most of the present ICT security control measures are only on an ad-hoc basis at best. There is therefore potential economic damage, which could result in the loss of strategic information, business interruption, loss of property, and liability claims. ICT security is an interdisciplinary process. It is more than just an information technology problem.

A systemic-holistic approach to this multi-disciplinary problem is proposed, where five organisations in Tanzania have been identified to be used as a case study and test bed at some stages of the study. Organisation **X** is among the five organisations to be included in this exercise.

1.2 How will the organisation benefit?

- The end result is a brief survey report that gives an estimate of the ICT security state in the Organisation and the consequences of losses for the organisation's value.
- The survey report will assist in designing and developing countermeasures tailored to the organisation that will remedy vulnerabilities and deficiencies identified during the survey.

1.3 Instructions for the questionnaire:

1. Spend a few minutes thinking about your organisation's mission and then focus on the ICT assets that are used to help the organisation fulfil its mission. An asset is something of value to the organisation.

   ICT assets can fall into the following categories:

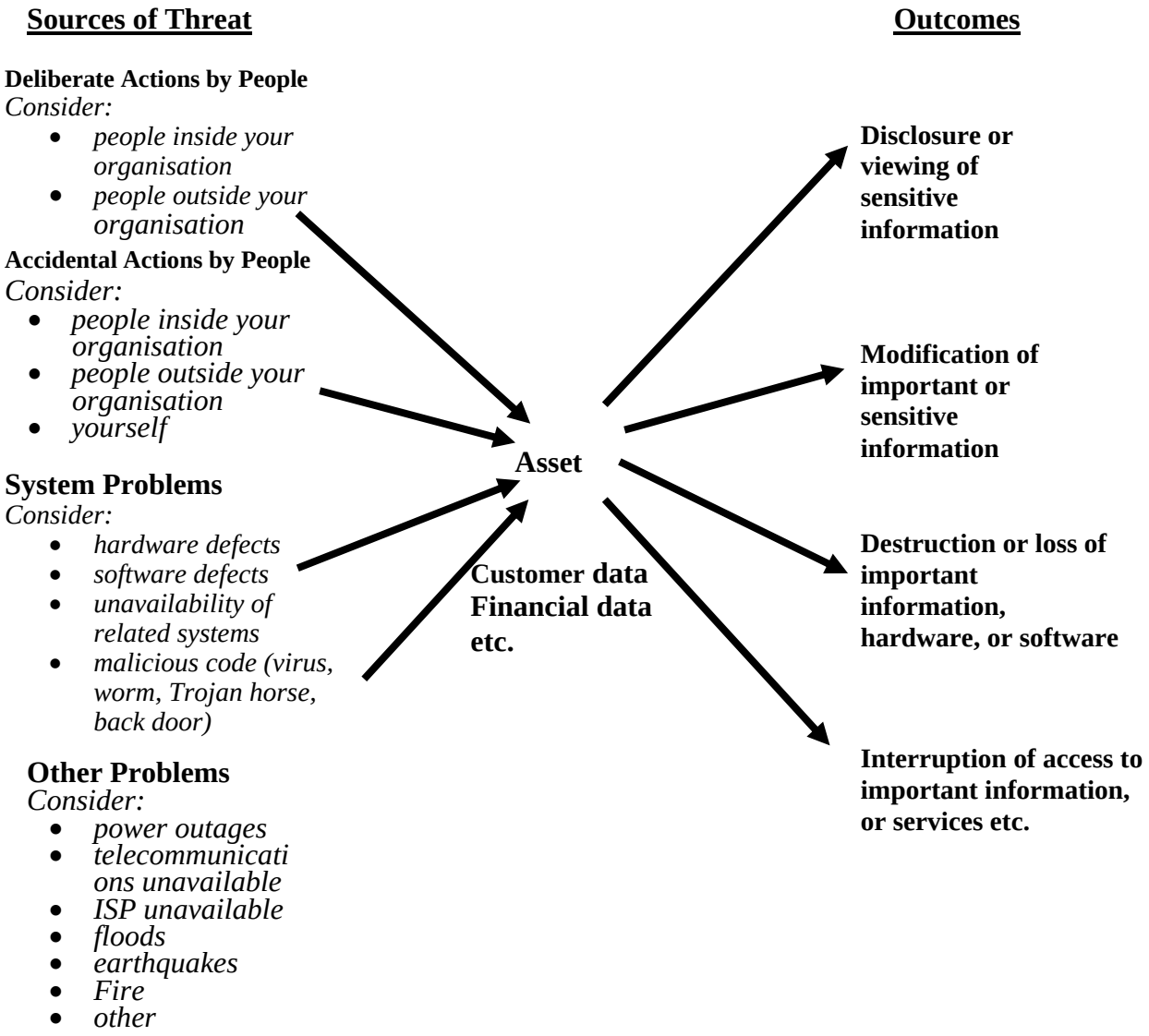
   - Information— documented (paper or electronic) information or intellectual assets/ intellectual property that is owned by Organisation **X** like customers data, trade secrets, manuals, policies, financial data, reports, investments, etc.
   - Systems— Information systems that process, transmit and store information. Thus software, hardware, personnel and management together form the system.
   - Software— Applications and services like operating systems, databases, networking software, other enterprise applications, etc., used for processing or transmission of information.
   - Hardware—Physical assets like servers, CD's, hard disks, routers, switches, etc, which are used by the organisation for transmission, storage or processing of data or information.
   - People— Expertise in the organisation, knowledge and experience which can be hard to replace.

   An example of areas of concern is presented on the next page

2. Answer each question to the best of your knowledge in terms of how the practice is currently used in your organisation, answering the multiple choice questions as follows:
   - If the practice is always or nearly always used, circle "Yes"
   - If the practice is not used, circle "No"
   - If the practice does exist but not used very much, not documented and not communicated to staff, or used by some department or individuals only, circle "Ad-hoc"
3. If likely answers are itemised, please tick the most appropriate answer.
4. In some cases you are asked to circle the right answer and, in others, space is provided for you to write an answer. Should there not be enough space for your answer, please include an additional sheet of paper and attach it to the questionnaire when handing it back.

1.4 An example of areas of Concern

What scenarios threaten your important assets?



Where the risks come from:

- **Can strike from ANYWHERE (inside the organisation OR from outside)**
- **Information is the most valuable asset and is the only commodity that can be stolen without being taken!**

Implications if not taken care of:

Service interruption
Consequential liabilities
Loss of Property
Loss of Reputation/Credibility etc.

Source: (Alberts & Dorofee, 2003, pp. 368)

Appendix B

Appendix B – Interview guide for Top Management

Top Management

Name (optional): _____ Date: _____

Organisation/Department Name (Optional): _____

Position: _____

SM1. What are the main/core services of the organisation? Please list at most 5 in order of importance.

No.	Name of the Core service
1	
2	
3	
4	
5	

SM2. To what extent are the functions of the core business/services computerised in your organisation?

Please give approximate percentage (*Use the list below to fill in the Percentage)*

Core services No.	Percentage

a. Not Computerised (Only e-mails services and secretarial work)
b. Between 1% – 20%
c. Between 21% - 40%
d. Between 41% - 60%
e. Between 61% - 80%
f. Between 81% - 100%

SM3. What percentage of the total budget of the organisation is allocated to Information and Communication Technology (ICT)? Please circle the letter which applies.

a. None
b. Between 0% – 2%
c. Between 3% - 5%
d. Between 6% - 8%
e. Between 9% - 11%
f. Between 12% - 14%
g. Between 15% - 16%
h. Above 17%, please state how much if you have the figure.

SM4. What percentage of the budget quoted above is allocated to ICT Security? Please circle the letter which applies.

a. Between 1% – 10%
b. Between 11% - 20%
c. Between 21% - 30%
d. Between 31% - 40%
e. Between 41% - 50%
f. Between 51% - 60%
g. Between 61% - 70%
h. Between 71% - 80%
i. Above 80%, please state how much if you have the figure.
j. None
k. Don't know

SM5. How do you rate your computer knowledge (please circle only one)

a. Excellent **b**. Very good **c**. Good **d**. Average **e**. Below average

SM6. How do you rate your ICT security awareness (please circle only one)

a. Excellent **b.** Very good **c.** Good **d.** Average **e**. Below average

SM7. Do the organisation's business strategies routinely incorporate ICT security considerations?

SM8. In your organisation what do you consider are the consequences of potential damage due to ICT risks, for the organisation? Please select what is applicable and indicate the level of damage exposure in the small box *(High [4], Medium-High [3], Medium [2] or Low [1]).*

A. Liability

1. Business Interruption ☐
2. Fraud & Embezzlement ☐
3. Robbery & Theft ☐
4. Defamation ☐
5. Infringement of Privacy ☐
6. Infringement of Trademark, © etc.☐

B. Loss of Property

1. Fraud & Embezzlement ☐
2. Robbery & Theft ☐

C. Business Interruption

1. Loss of sales ☐
2. Extra expenses ☐

SM9. Does the organisation take steps to minimise the consequences of ICT risks?

_____

SM10. Do you have any other opinions/issues or suggestions/comments regarding the information systems management in your organisation, and in particular information security?

_____
_____
_____

Thank you very much for your valuable time!

Appendix C

Appendix C – Interview guide for operational Management

Operational Management

Name (optional): _____ Date: _____

Organisation/Department Name (Optional): _____

Position: _____

OM1. What are the main/core services of the department/directorate? Please list at most 5 in order of importance.

No.	Name of the Core service
1	
2	
3	
4	
5	

OM2. To what extent are the functions of the core business/services computerised in your department/directorate?

Please give approximate percentage (*Use the list below to fill in the Percentage)*

Core services No.	Percentage

a. Not Computerised (Only e-mail services and secretarial work)
b. Between 1% – 20%
c. Between 21% - 40%
d. Between 41% - 60%
e. Between 61% - 80%
f. Between 81% - 100%

OM3. What percentage of the total budget of the department is allocated to Information Communication Technology (ICT)? Please circle the letter which applies.

a. None
b. Between 0% – 2%
c. Between 3% - 5%
d. Between 6% - 8%
e. Between 9% - 11%
f. Between 12% - 14%
g. Between 15% - 16%
h. Above 17%, please state how much if you have the figure.
i. Don’t know

OM4. What percentage of the ICT budget quoted above is allocated to ICT Security? Please circle the letter which applies.

a. Between 1% – 10%
b. Between 11% - 20%
c. Between 21% - 30%
d. Between 31% - 40%
e. Between 41% - 50%
f. Between 51% - 60%
g. Between 61% - 70%
h. Between 71% - 80%
i. Above 80%, please state how much if you have the figure.
j. None
k. Don't know

OM5. How do you rate your computer knowledge (please circle only one)

a. Excellent
b. Very good
c. Good
d. Average
e. Below average

OM6. How do you rate your ICT security awareness (please circle only one)

a. Excellent
b. Very good
c. Good
d. Average
e. Below average

OM7. Does the department have information security policies and regulations in place? ____ Is it periodically reviewed?____ Is it communicated to staff?___ When was it last updated?_____

OM8. Do Staff members understand their ICT security roles and responsibilities?____ If your answer is yes, please indicate if they are **documented and enforced**._____

OM9. Does your department asses risks to information systems security?____ If so, How frequently_____

OM10. Is security awareness, training, and periodic reminders, concerning the information systems provided for all personnel? _____. If **yes**, when was the last training/awareness seminar?_____

OM11. In your department/organisation, what do you consider are the consequences of potential damage due to ICT risks? Please select what is applicable and indicate the level in the small box *(High [4], Medium-High [3], Medium [2] or Low [1])*

A. Liability
1. Business Interruption ☐
2. Fraud & Embezzlement ☐
3. Robbery & Theft ☐
4. Defamation ☐
5. Infringement of Privacy ☐
6. Infringement of Trademark, © etc.☐

B. Loss of Property
1. Fraud & Embezzlement ☐
2. Robbery & Theft ☐

C. Business Interruption
1. Loss of sales ☐
2. Extra expenses ☐

OM12. What damage associated with ICT risks has the department/directorate (main/core services/units of the organisation) experienced? Are there any records? (see sample below)

YEAR	Damage	Cause	Effect
1998-2000			
2001-2003			
2004			

Possible Damage
1. Business Interruption
2. Liability
3. Loss of Property (Fraud, robbery), Loss of critical information etc.

Possible causes
1. System failure
2. Power fluctuations /outage
3. Virus/Worm
4. Sabotage
5. Hacking
6. Disgruntled employee/s misuse their privileges/rights in the system

Possible effects
1. Loss of reputation/customer confidence
2. Loss of sales/earnings
3. Liability claims (E.g. Fines/legal penalties)
4. Financial: Extra expenses (e.g. using temps for records recovery, adding software to deter further intrusions)
5. Fraud and embezzlement or cheating

OM13. Does the organisation/department take steps to mitigate the consequences of ICT risks? Have any countermeasures/initiatives already been introduced for the above Loss exposures? (E.g. creating/enforcing ICT security policy), please indicate them_____

OM14. Do you have any other opinions/issues or suggestions/comments regarding the information systems management in your organisation, and in particular information security?

_____
_____
_____

Thank you very much for your valuable time!

Appendix D

Appendix D - Interview guide for Operational/Technical Management

Operational Management – IT Department

Name (optional): _____ Date: _____

Organisation/Department Name (Optional): _____

Position: _____

SIT1. What are the main/core services of the department?

No.	Name of the Core service
1	
2	
3	
4	
5	

SIT2. What is the number of computers in use in the entire organisation (estimate):_____

SIT3. How many of these are connected to the corporate network _____

SIT4. How does your network infrastructure interconnect the branches/departments? (E.g. if you have a LAN which is interconnected using Wireless, Fibre, VPN through the public/infrastructure provider) Do you allow remote access?

SIT5. What are the main/core services of the organisation? Please list at most 5 in order of importance. [Follow up question from the senior management]

No.	Name of the Core service
1	
2	
3	
4	
5	

SIT6. To what extent are the functions of the core business/services computerised in your organisation in approximate percentages? (*Use the list below to fill in the Percentage)*

Core services No.	Percentage

a. Not Computerised (Only e-mails services and secretarial work)
b. Between 1% – 20%
c. Between 21% - 40%
d. Between 41% - 60%
e. Between 61% - 80%
f. Between 81% - 100%

SIT7. In what computer systems are these core services running? (e.g. mainframe computer systems, Windows based). What communication protocols are in use (e.g. Interoperable protocol suit TCP/IP etc.)

SIT8. What percentage of the total budget of the organisation is allocated for ICT?
a. None
b. Between 0% – 2%
c. Between 3% - 5%
d. Between 6% - 8%
e. Between 9% - 11%
f. Between 12% - 14%
g. Between 15% - 16%
h. Above 17%, please state how much if you have the figure.

SIT9. What percentage of the ICT budget quoted above, is allocated for ICT Security?_____
a. Between 1% – 10%
b. Between 11% - 20%
c. Between 21% - 30%
d. Between 31% - 40%
e. Between 41% - 50%
f. Between 51% - 60%
g. Between 61% - 70%
h. Between 71% - 80%
i. Above 80%, please state how much if you have the figure.
j. None
k. Don't know

SIT10. How many full-time ICT staff are employed by your organisation? _____

SIT11. Do you have a special division/unit dealing with ICT security? **(YES/NO)**

SIT12. If the answer to **SIT 10 is No**, How many full-time central ICT security staff are employed by your organisation?

a. None
b. One
c. Two
d. Three
e. More than three, please specify.

SIT13. How do you rate your computer knowledge (please circle only one)

a. Excellent
b. Very good
c. Good
d. Average
e. Below average

SIT14. How do you rate your information technology security awareness? (please circle only one)

a. Excellent
b. Very good
c. Good
d. Average
e. Below average

SIT15. Does the department have information security policies and regulations in place? ____ Are they periodically reviewed?____ Are they communicated to staff?___ When were they last updated?_____

SIT16. Do Staff members understand their ICT security roles and responsibilities?____ If your answer is yes, please indicate if they are **documented and enforced**._____

SIT17. Does your department asses risks to information systems security?____ If so, How frequently_____

SIT18. Are the Security awareness, training, and periodic reminders, concerning the information systems provided for all personnel? _____. If **yes**, when was the last training/awareness seminar?_____

SIT19. Is there adequate in-house expertise for all supported services, mechanisms and technologies?

_____

SIT20. In your department/organisation, what do you consider are the consequences of potential damage due to ICT risks? Please select what is applicable and indicate the level in the small box *(High [4], Medium-High [3], Medium [2] or Low [1])*

A. Liability
1. Business Interruption ☐
2. Fraud & Embezzlement ☐
3. Robbery & Theft ☐
4. Defamation ☐
5. Infringement of Privacy ☐
6. Infringement of Trademark, © etc.☐

B. Loss of Property
1. Fraud & Embezzlement ☐
2. Robbery & Theft ☐

C. Business Interruption
1. Loss of sales ☐
2. Extra expenses ☐

SIT21. What damage associated with the ICT risks has the department/directorate (main/core services/units of the organisation) experienced? Are there any records? *(see example below)*

YEAR	Damage	Cause	Effect	Frequency
1998-2000				
2001-2003				
2004				

Possible Damage
1. Business Interruption
2. Liability
3. Loss of Property (Fraud, robbery)
4. Specific examples;
   a. System not functioning as expected
   b. Customer database/information compromised
   c. Fraud in the information systems
   d. Back-up damaged
   e. Loss of critical information

Possible causes
1. System failure
2. Power fluctuations /outage
3. Virus/Worm
4. sabotage
5. Hacking
6. Disgruntled employee/s misuse their privileges/rights in the system
7. Denial of service attack
8. Human error

Possible effects
1. Loss of reputation/customer confidence
2. Loss of sales/earnings
3. Liability claims (E.g. Fines/legal penalties)
4. Financial: Extra expenses (e.g. using temps for records recovery, adding software to deter further intrusions)
5. Frauds and embezzlement or cheating

SIT22. Does the organisation take steps to minimise the consequences of ICT risks? If there are any countermeasures/initiatives so far for the above Loss exposures indicate them. (E.g. creating/enforcing ICT security policy).

_____

SIT23. If the answer to question No. **SIT21 is Negative**, when do you intend to implement your ICT security solution?: within

(a) 0-6 months
(b) 6-12 months
(c) 13- 24 months
(d) Don't know

Section B

Practice	Is this practice used by your organisation?
Security Strategy	
SIT24. The organisation's business strategies routinely incorporate ICT security considerations.	**Yes No Ad-hoc**
SIT25. ICT Security strategies and policies take into consideration the organisation's business strategies and goals.	**Yes No Ad-hoc**
SIT26. ICT Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organisation.	**Yes No Ad-hoc**
Security Management	
SIT27. The organisation's hiring and termination practices of staff take information security issues into account.	**Yes No Ad-hoc**
SIT28. Management receives and acts upon routine reports summarising security-related information (e.g., audits, logs, risk and vulnerability assessments).	**Yes No Ad-hoc**
Collaborative Security Management?	
SIT29. The organisation has policies and procedures for protecting information when working with external organisations (e.g., third parties, collaborators, subcontractors, or partners).	**Yes No Ad-hoc**
Is there any Contingency Planning/Disaster Recovery? (YES/NO)	
SIT30. A critical analysis of operations, applications, and data has been performed.	**Yes No Ad-hoc**
SIT31. The organisation has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	**Yes No Ad-hoc**
SIT32. The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	**Yes No Ad-hoc**
SIT33. All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	**Yes No Ad-hoc** **Yes No Ad-hoc**

Physical Security Plans and Procedures			
SIT34. There are documented policies and procedures for managing visitors.	**Yes**	**No**	**Ad-hoc**
SIT35. There are documented policies and procedures for physical control of hardware and software.	**Yes**	**No**	**Ad-hoc**
Physical Access Control			
SIT36. There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	**Yes**	**No**	**Ad-hoc**
SIT37. Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorised access.	**Yes**	**No**	**Ad-hoc**
Monitoring and Auditing Physical Security			
SIT38. Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.	**Yes**	**No**	**Ad-hoc**
System and Network Management			
SIT39. Sensitive information is protected by secure storage (e.g., **backups stored off site**, **discard process for sensitive information).**	**Yes**	**No**	**Ad-hoc**
SIT40. The integrity of installed software is regularly verified.	**Yes**	**No**	**Ad-hoc**
SIT41. All systems are up to date and with respect to **revisions, patches**, and recommendations by security advisors.	**Yes**	**No**	**Ad-hoc**
SIT42. There is a documented and tested data backup plan for backups of both software and data. All responsible staff understand their responsibilities under the backup plans.	**Yes**	**No**	**Ad-hoc**
SIT43. As IT staff member, do you follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges? • Default accounts and default passwords have been removed from systems.	**Yes**	**No**	**Ad-hoc**
SIT44. Only necessary services are running on systems (computers and servers) – all unnecessary services have been removed.	**Yes**	**No**	**Ad-hoc**
Monitoring and Auditing IT Security			
SIT45. System and network monitoring and auditing tools are routinely used by the organisation. Unusual activity is dealt with according to the appropriate policy or procedures.	**Yes**	**No**	**Ad-hoc**
SIT46. Are firewall and other security components periodically audited for compliance with policy?	**Yes**	**No**	**Ad-hoc**
Authentication and Authorization			
SIT47. Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	**Yes**	**No**	**Ad-hoc**
SIT48. Are there any documented policies and procedures to establish and terminate the right of access to information for both individuals and groups?	**Yes**	**No**	**Ad-hoc**

SIT49. Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorised manner. Methods or mechanisms are periodically reviewed and verified.	**Yes**	**No**	**Ad-hoc**
Vulnerability Management			
SIT50. Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	**Yes**	**No**	**Ad-hoc**
Encryption			
SIT51. Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).	**Yes**	**No**	**Ad-hoc**
Incident Management			
SIT52. Do any documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations?	**Yes**	**No**	**Ad-hoc**
SIT53. Are Incident management procedures periodically tested, verified, and updated?	**Yes**	**No**	**Ad-hoc**

SIT54. Do you have any other opinions/issues or suggestions/comments regarding the information systems management at your organisation, and in particular information security?

_____

_____

_____

Thank you very much for your valuable time!

Appendix E

Appendix E – Interview guide for General staff and Technicians

General & technical staff

Name (optional): _____ Date: _____

Organisation/Department Name (Optional): _____

Position: _____

GS1. What are your responsibilities within the department?

_____
_____
_____
_____

GS2. How do you rate your computer knowledge (please circle only one)

a. Excellent
b. Very good
c. Good
d. Average
e. Below average

GS3. How do you rate your information technology security awareness (please circle only one)

a. Excellent
b. Very good
c. Good
d. Average
e. Below average

GS4. Do you understand your information technology security roles and responsibilities? If the answer is yes, Please indicate if they are documented or not._____

GS5. Are the Information Security awareness, training, and periodic reminders, provided for all personnel. If **YES**, when was the last training/awareness seminar?

GS6. Are you aware of any existing information systems security policies in the department?

GS7. If the answer to question No. **GS6 is Positive.** Does the department continuously enforce and monitor its security policies. (If the answer is **YES**, any examples?)

GS8. Have you ever been affected by a virus? On what system were you affected? Windows 95, Windows 98, Windows 2000, Windows XP, Linux, Macintosh, other system?

GS9. How, do you believe, was the Virus introduced - through the Internet, through a diskette, through a game program, other?

GS10. How regularly is your Ant-Virus software updated in your PC?

a. When there is a problem
b. It is automated
c. Technical staff pass around and assist in updating (How frequently?)
d. Not scheduled

GS11. How regularly is your operating system patched/updated in your PC?

a. When there is a problem
b. It is automated
c. Technical staff pass around and assist in updating (How frequently?)
d. Not scheduled

GS12. What damage/problems/s associated with ICT risks has the department (main/core services/units of the organisation) experienced? Are there any records?

YEAR	**Damage/s (Problems)**	**Cause**	**How long did it take to recovery from the problem? (1 hour, day, week or month)**	**How frequently**
1998-2000				
2001-2003				
2004				

Possible Damages (Problems)

1. System not functioning as expected
2. Customer database/information compromised
3. Fraud in the information systems
4. Back-up damaged
5. Denial of service
6. Others, please list

Possible causes

1. System failure
2. Power fluctuations /outage
3. Virus/Worm
4. sabotage
5. Hacking
6. Disgruntled employee/s misuse their privileges/rights in the system

GS13. Do you have any other opinions/issues or suggestions/comments regarding the information systems management at your organisation, and in particular information security?

_____
_____
_____

The following questions were specific to staff from the IT department

GS14. Do you have corporate anti-virus software? **(YES/NO)**

GS15. What does your anti-virus software protect?

a. PCs
b. Servers
c. Gateways
d. All

GS16. Has your organisation installed an intrusion detection system? **(YES/NO)**

GS17. Has your organisation installed a firewall? **(YES/NO)**

GS18. Do you monitor/block unproductive web browsing? **(YES/NO)**

GS19. Is there a policy for web/email usage? **(YES/NO)**

GS20. How frequently do you carry out back-up for information systems

a. Daily
b. Weekly
c. Monthly
d. Never
e. Not scheduled
f. Hourly, please specify

Thank you very much for your valuable time!

Appendix F

Appendix F: ICT in Tanzania

1. Introduction

Tanzania is the biggest of the East African countries (i.e. Kenya, Uganda and Tanzania) with an approximate area of 945,000 km^2 and an estimated population of 33 million people according to the 2002 census and an average growth rate of 2.8%. About 50% of the population is living below the poverty line. Per capita Gross Domestic Product (GDP) is estimated at US$ 251 (2001) (Tanzania, 2005). Continued donor assistance and solid macroeconomic policies supported real GDP growth of more than 5.2% in 2004 (cia, 2005).

1.1 Background

Sometimes it is important to understand history first, in order to understand the nature of the problem. This section begins by tracing the history of ICT in Tanzania. It was not until 1965[1] when the first computer, named the ICT1500, was imported into the country and installed in the Ministry of Finance. Later on, the Ministry acquired a new computer, an ICL 1900, and by 1974 a total of 7 computers were in the country. Even this gradual increase in the number of computers was not without problems. Among the major problems was that of installation. The whole process of installation was entirely dependent on foreign experts who in some cases were not adequately qualified or experienced. The applications were not properly documented and for that reason they could only run in their presence. In the early 1970s, the Ministry found the need to computerise the whole accounting system of the government by using an ICL 1900 that was located at the Ministry's headquarters in Dar-es-Salaam. Given the size of Tanzania and its undeveloped communications network at that time, it rendered it impossible to use a centralised card-based computer to process all government accounts. The project failed and was abandoned after incurring heavy losses. This marked the second reason for the project failure – uncoordinated planning (Suluo, 2003; Drew & Foster, 1994).

According to (Suluo, 2003), other computers which were later installed at the Tanzania Electricity Supply Company (TANESCO), the State Trading Corporation (STC), the National Bank of Commerce (NBC), and elsewhere, which were required to handle the extra computing service demands of other public institutions. However, later on, the State Trading Corporation (STC) and other organisations also suffered the consequences arising from the problems concerning installation, maintenance, management and uncoordinated planning. These consecutive failures resulted in heavy financial loss and consequently the government faced severe criticism from both the members of parliament and the general public. As a result, in 1974, the government banned the importation of computers and all related equipment into Tanzania.

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

An increase in the number of microcomputers due to technology advancement and the collapse of the East African Community (Tanzania, Uganda and Kenya) were among the several factors leading to the opening of the doors for the importation of computers in the early 1980s. Computers were then ordered by private companies and individuals from their own private funds and with the permission of the government for every importation (Drew & Foster, 1994).

1.2 The situation of ICT from the Nineties to date

The significant achievement of ICT in Tanzania can be traced from the early nineties when the ban was lifted, 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, made more complicated by user's 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 (Odedra & Madon, 1993). In 1994, the first TV station started broadcasting, with the establishment of mobile phone companies in 1995, and Tanzania was connected to the Internet for the first time in 1996 (MEA, 2001; Casmir & Yngström 2003). Although access to ICT was still on the lower side compared with developed countries, there were signs of better accessibility to various communication devices such as TVs, Radios, Telephones and Personal Computers as show in table 1 below.

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]

The adjustments on policy also include tax exemption on PCs and their accessories after which there was quite a lot of improvement in ICT usage as depicted in table 2, which gives some of the key ICT statistics indicators in Tanzania.

Table 2: Key ICT statistics indicators in Tanzania

Indicators	1961	1993	2002	2006
Fixed line exchange capacity	11,300	125,703	234,640	236,989
Mobile operators		1	4	5
Mobile subscribers		1,500	700,000	3,855,190
Teledensity (lines per 100 people)	0.1	0.32	1.22	11
Data communications operators (currently known as Service Application Operators)			16	24
Internet service providers		1	23	25
Internet subscribers (Dial-up accounts and Wireless)		10	14,000	
Internet capacity (Total bandwidth Kbits)		64	44,000	
Television licences		1	24	29
Radio broadcast licences	1	2	18	47

Source: Tanzania National ICT Policy (TzICT, 2003; TCRA, 2006)

ICT – Current status

At the individual level, people are purchasing computers for home use, getting dial-up connections, as well as enrolling in short courses on how to use PCs. At 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 and organisations in general are changing from manual to computerised systems, while on the street the number of Internet cafes is increasing.

The survey conducted in 2001 in Tanzania, to find out the status of the ICT in organisation X (one of the studied organisations) which is typically a large non-commercial organisation, showed that the number of computers had increased by more than 8 times 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 at that time. The results indicated different brands of PCs running on top of different operating systems ranging from Disk Operating System (DOS), various versions of Windows and various versions of Linux, Macintosh, etc. Although the study indicated that most of these PCs were bought with UPS or power stabilisers, most of these were malfunctioning due to power fluctuations. Power fluctuation accounted for more than 24.2% of all problems in ICT equipment reported to the organisation's IT unit. Viruses were found to be the main source of problems 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 an increase in service unavailability time. Furthermore, the power fluctuations have been the 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 (Bakari & Mboma, 2001). Generally at the organisational level, computerisation of core business operations is advancing.

At the national level, a national ICT policy was put in place (in 2003) and various organisations in the public and private sector are now in the process of computerisation. There are number of initiatives at the national level including, for example: the Agricultural Information Management Database, Land Information Management Database, The Tanzania Inter-Bank Settlement Systems, Natural Resources and Tourism Management Information Systems; Customs Administration System (ASYCUDA++); Online Motor Vehicle Registration System; Strategic Budget Allocation System (SBAS) for the Ministry of Finance; By-Law making database for Local Authorities; Education Information Management System (EIMS); The Local Government Monitoring Database system (LGMD); Integrated Financial Management System (IFMS); an accounting system for central and local Governments, Integrated payroll and Human Resources Information System, Planning and Reporting Database (PlanRep) for the Local Government Authorities throughout the country; Integrated Statistical Database; the recent National Identification Card Project, announced by the government through the local news papers http://www.dailynews-tsn.com/page.php?id=5651, just to mention a few. The financial industry is also advancing, as most of them, such as banks, are computerised, with the introduction of Automated Teller Machines (ATM) and Point of Sale (POS) machines. In general there are a number of on-going initiatives in many sectors to make use of ICT in the country.

Connectivity[2]

There are also some other initiatives when it comes to the National Backbone infrastructure. Currently, the existing Optic Fibre Cable (OFC) transmission networks are privately operated by TRC, TAZARA, TANESCO and SONGAS, while the Microwave radio systems are mainly operated by TTCL and mobile cellular companies such as Tigo Ltd, Vodacom (T) Ltd, Celtel (T) Ltd and Zantel. In addition, in the region, in particular in the East African Community and Southern African Development Community (SADC) to which Tanzania belongs, we have the proposed East African Sub-marine Cable System (EASSY) project. This project aims at providing good quality, high capacity optic fibre for international connectivity from Tanzania, to within Africa and the rest of the world, thereby reducing the current high cost of using satellite telecommunication facility providers. Currently, the only way for East African countries to gain access internationally is via satellites. The EASSY project intends to implement a 9,900 Km submarine optical fibre cable system that will link the whole of the Eastern Africa Seaboard starting at Mtunzini near Durban in South Africa, continuing on Northwards, branching out to Maputo in Mozambique, Mahajanga in Madagascar, Dar es Salaam and Zanzibar in Tanzania, Mombassa in Kenya and terminating at Djibouti and Port Sudan. Provision is also made for the cable to provide branching to Mogadishu in Somalia. Eastern Africa hinterlands and land-locked countries will be able to access the proposed EASSY system at the cable's appropriate shore landing stations at Mtunzini, Maputo, Mahajanga, Dar es Salaam, Mombassa, Mogadishu, Djibouti and Port Sudan.

[2] Technical Report on Feasibility Study for Implementation of The National ICT Backbone Infrastructure, .MINISTRY OF COMMUNICATIONS AND TRANSPORT, United Republic of Tanzania), June, 2005. Available at http://www.moct.go.tz/documents/ (Accessed on December, 2006)

Conclusion

It is not my intention to explore the whole list of ICT initiatives in Tanzania. These are just a few examples to give an indication of ICT development. But I would like to conclude this section by highlighting one important observation. Throughout the study, one of the general observations made in the studied environment is that the problem of maintenance, management and uncoordinated planning of ICT as observed by Suluo (2003) and Drew & Foster (1994) way back in 1974, still exist. In my opinion this may even complicate further the ICT security management problem if it not addressed, because we have two problems here, first that of general management of ICT and secondly that of ICT security.

Appendix G

Appendix G: Case 1 - BRITS Processes when applied to non-commercial Organisations

1. Introduction

As pointed out in the introduction, the dependence on ICT to run core services in many organisations today is increasing. Moreover, the ability of an organisation to achieve its mission and meet its business objectives is directly linked to the state of its information systems, whose assets are intangible by nature [Alberts & Dorofee, 2003]. Systems store, process, and transmit the critical information that drives an organisation's services. ICT-dependent organisations must therefore have financial protection against ICT risks. The reason for this is that these organisations' goals will most likely be more affected by the financial consequences of ICT risks than by traditional risks like fire, for instance. The purpose of BRITS was to reach this objective by financially protecting organisations from the consequences of ICT risks [Magnusson, 1999].

BRITS consists of four elements, namely shareholder value, risk transfer, IT and IT-security and the knowledge gateway is the interface between these elements. According to Magnusson, the gateway (see Figure 1 below) translates financial damage exposures into IT security properties, and vice versa. He ascertains that the protection against ICT risks and investment in ICT security should be viewed in the context of shareholder value.

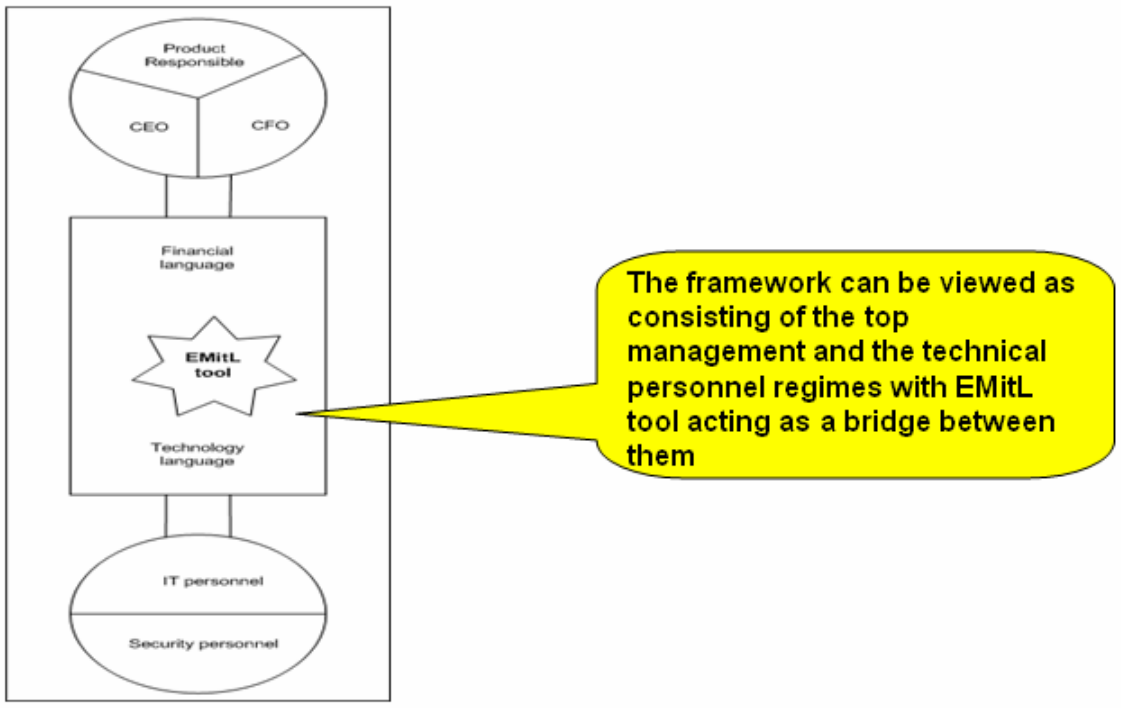


Figure 1: The knowledge Gateway, Source [Magnusson, 1999, Pp. 141]

It is also argued in BRITS that a lack of common terminology between decision makers with a financial background and the ICT security experts can lead to sub-optimisation of ICT security measures if the existing knowledge gap is not filled.

Originally BRITS was developed for commercial organisations and tested in commercial organisations in the developed countries as summarised in Figure 2 below.

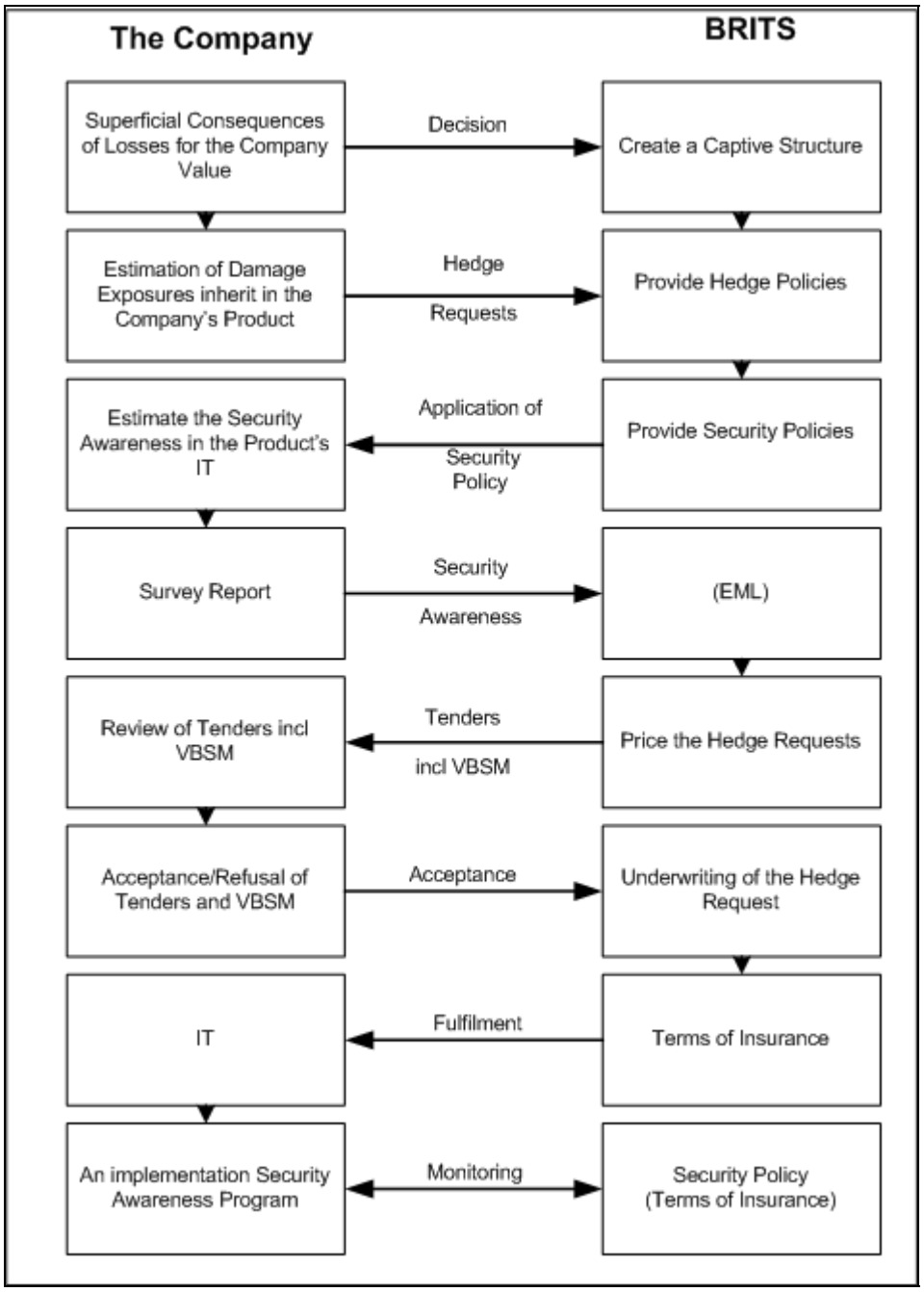


Figure2: The original BRITS process (Source: [Magnusson, 1999, Pp. 123])

We could not therefore deploy the framework as it is in the non-commercial organisations. The first task was therefore to customise it, so that it could be used in non-commercial organisations in the developing countries. Figure 3 summarises the customised BRITS processes to be applied to non-commercial organisations. There are two major issues to note in the customisation/transformation. First the language

used needed to be changed from that of business to that of services and secondly and most important was the exclusion of the insurance part. This was due to the fact that in developing countries most non-commercial organisations' dependence on ICT to run their core services is in its infancy.

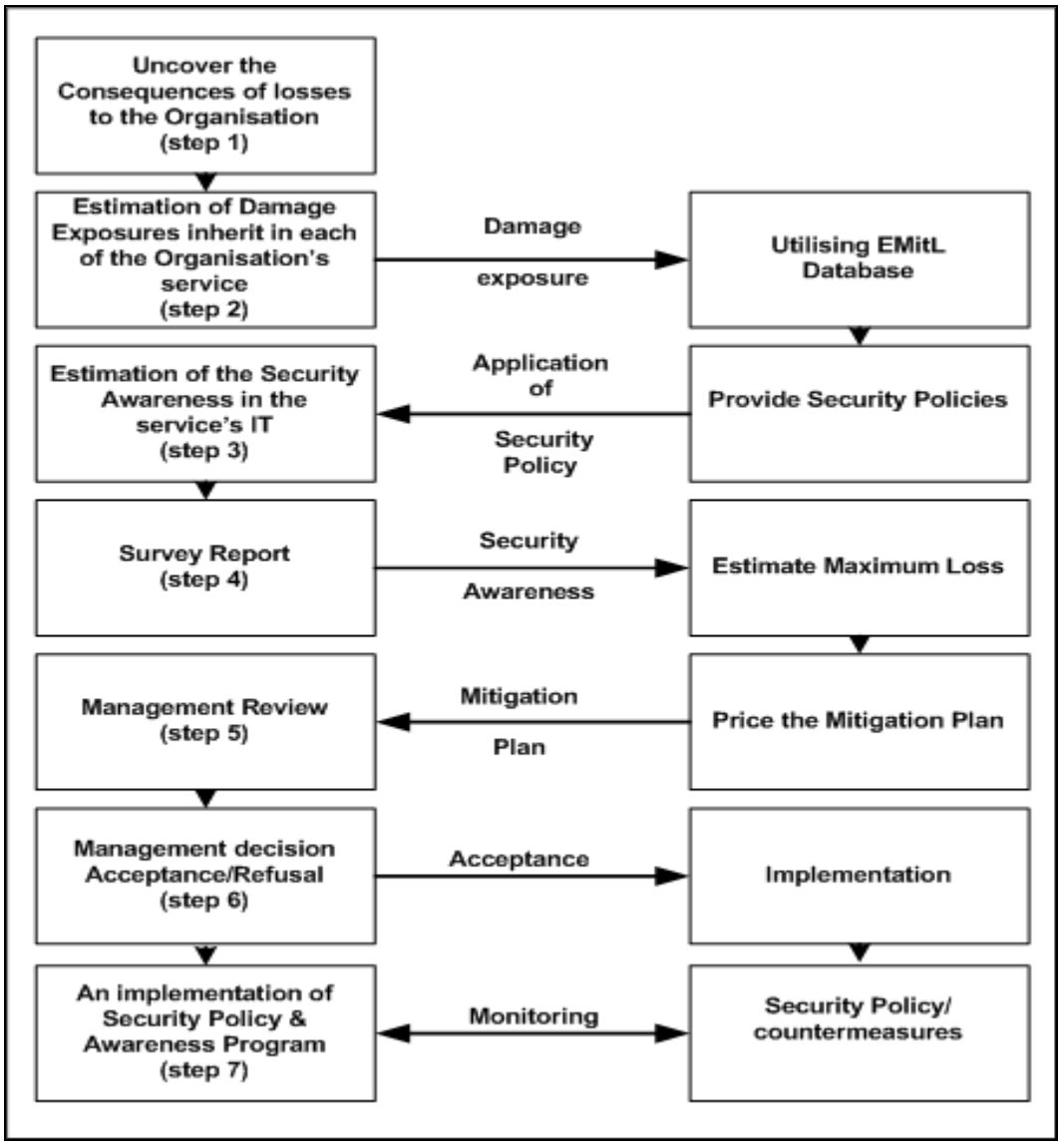


Figure 3: Customised BRITS Process for application to non-commercial organisations

The next section details the steps of the customised BRITS process applied to the non-commercial organisations.

2. The Process of BRITS customised for application to non-commercial organisations

As indicated in figure 3 above, the customised BRITS framework consists of seven (7) steps as described below.

2.1 First step – Uncover the consequences of losses to the organisation

BRITS uses a top-down approach. The top management have to be convinced that their organisation is vulnerable to ICT-related risks. The original BRITS financial indicators were used to estimate the consequences of losses in the company's value. This estimation was based on three groups of damage exposures due to ICT risks, namely liability claims, direct loss of property and business interruption, in our case service interruptions. In the same way, in non-commercial organisation the question to be answered during this stage is how this damage exposure could affect the organisation. In practice, a quick scan of what the organisation is doing and how its core services are linked to the use of ICT is recommended before a meeting with the top management. In order to capture this information, a consultation with the chief executive officer (CEO) is needed, together with the chief financial officer (CFO), IT managers and the heads of the units involved in the provision of the core services. A face-to-face interview with the respondents is recommended. To meet this objective in this research we used questionnaires presented in Appendices A to E.

Among other questions are what parameters are required for directly feeding into the EMitL database. In our work, these are question numbers 8 and 11 in the top management and operational management questionnaires respectively. If this question is answered correctly, the parameters collected could be used as input directly into the EMitL database. Perhaps it is important at this time to describe what EMitL is and its features, before we go ahead with the next step.

2.2 The Estimated Maximum information technology Loss (EMitL) database explained

The 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 cost of the loss exposure inherent in an organisation's service in a better way thereby be incorporating it into the organisation's service price. The EMitL database, which was developed using MS-Access, maps the different hedge policies with the security properties and levels. The security measures are grouped into four security levels, starting with security level 1 (low security) to level 4 (highest security). Figure 4 below shows a snapshot of the EMitL tool interface. In the figure, for example, the hedge policy 'Liability' for 'service interruption', 'Defamation', 'Infringement of Privacy' and Infringement of trademark' was the input. The level of protection required in this particular example is equivalent to the hedge level 2. Consequently, the output is a security policy against ('service interruption', 'Defamation', 'Infringement of Privacy' and Infringement of trademark') based on the adequate security measures at security level 2. Table 1 shows how these different damage exposures (in the form of a hedge policy) are mapped into the security properties categorised as integrity, confidentiality and availability.

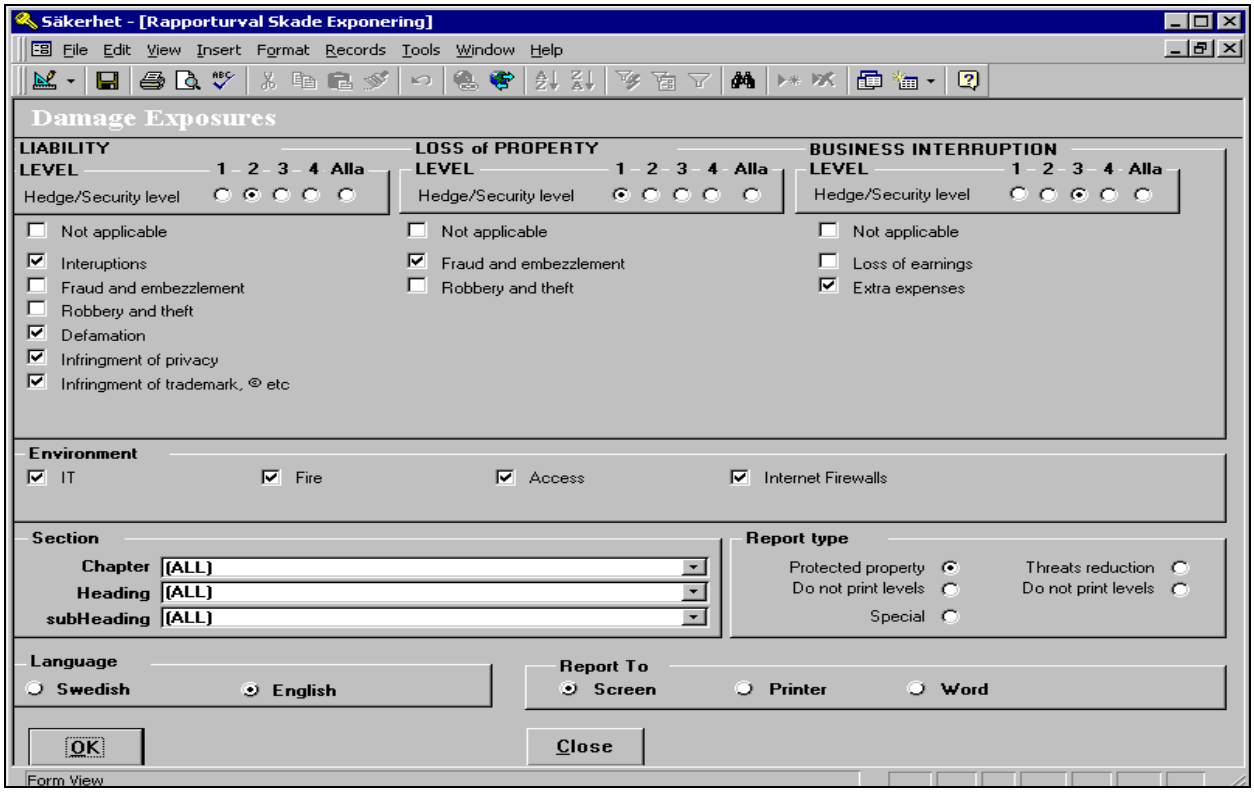


Figure 4: Snapshot of the EMitL database interface

In the framework, the damage exposures are divided into Liability, Loss of property and Service interruption. Liability exposure is further divided into liability damage due to service interruption, liability of loss of property (fraud, embezzlement, robbery and theft), infringement of privacy, defamation and infringement of copyright, trademark and patent. Loss of property consists of exposure to fraud, embezzlement, robbery and theft, and finally, Service interruption which may result in loss of earnings and extra expenses. Table 3-1 presents the damage exposure with the respective ICT security properties that are affected.

Table 1: Damage exposure and ICT security properties

Damage exposures	ICT security Properties		
	Integrity	Availability	Confidentiality
Liability			
Service Interruption		**x**	
Fraud & Embezzlement	**X**		
Robbery & Theft			**X**
Defamation	**X**		
Infringement of Privacy			**X**
Infringement of Trademark, © etc.	**X**		
Loss of Property			
Fraud & Embezzlement	**X**		
Robbery & Theft			**X**
Service Interruption		**X**	

Source: [Magnusson, 1999, P. 143]

The EMitL database is also conceptually structured into three groups; logical, physical and organisational as follows;

(i) Logical security measures include;
   a. Measures against masquerade and illegal login render it more difficult for unauthorised entities (users or programs) to pretend to being a different entity, and thereby bypass or circumvent the rules of the authentication mechanism.
   b. Protection of accountability or non-repudiation which obstructs users from falsely denying that they have either originated or received messages or transactions.
   c. Access control measures which reduce the risk of unauthorised entities (users or processes) getting access to system programs, applications and data.
   d. Protection of routing patterns
   e. Prevention against denial of service attacks.
   f. Measures against data and program modification, insertion or destruction.

(ii) Physical security countermeasures include;
   a. Power supply and Spare parts
   b. Fire protection.
   c. Prevention against water damage.
   d. Access and mechanical protection.

(iii) Organisational security countermeasures
   a. Roles and responsibilities
   b. Installation, configuration and operation of software and hardware.
   c. Protection of intellectual properties.

[Magnusson, 1999, P. 165-166]

The EMitL database has considered four levels of security which comprise the following IT areas;

(a) **User workstations:** Computers (such as PCs, PC notebooks and UNIX user workstations) that are physically accessible to the user and used by one person at a time as a stand-alone host or part of a computer network.
(b) **A Server:** Any computer that is not a single-user machine; others can share it.
(c) **Network applications:** Distributed applications or client/server applications.
(d) **Local area networks:** Networks that are geographically local and under the physical protection and administration of the organisation.
(e) **Remote connections:** Connections between local area networks and/or between geographically distant computers.
(f) **Common IT:** Besides the first five listed IT areas, the EMitL database has **common IT** security issues that cannot be referred to any specific technology area. They address the security measures shared between all IT areas. Organisational issues, user identities and user management, general access control and accountability principles are examples of common IT areas.

[Magnusson, 1999, P. 167-168]

The flexibility of the EMitL database allows for expansion of new IT areas as well. Therefore, the list of threats, weaknesses, vulnerabilities and countermeasures can be continuously updated to meet the current security requirements. It is also important to note that the database has two language options, Swedish and English.

2.3 Second step - Estimating damage exposure inherent in each of the organisation's services

Once the top management's attention has been gained, the next step is to estimate the damage exposure inherent in each of the organisation's core services.

2.4 Third step – Estimating the security awareness in the organisation

The outcome of the second step when running the database with the obtained parameters from the organisation is to set up security policies (countermeasures) which should have been in place given the input parameters provided to the database. The report can be exported to Word and printed as a document. An example of a page of such policies is indicated in the box below.

An example of page (7 out of 98 pages) of an output from the EMitL database

POSTEN **Damage**

User WorkStations

Physical Protection

Protection against Technical Errors, System, and Components Failures

Security Level 2

2010 The PC's and user workstations should be standard components that are built with standard components to make them easy to replace as a whole and to make it easy to replace spare parts without delay.

Property protected: Availability

2020 If the user workstation is not a standard component there should be strong reasons for its use, and service contracts covering the hardware must be in effect.

Property protected: Availability

Physical Access Control

Security Level 1

2040 Protection of the property, with unique marking of all equipment. Special protection for portable equipment is

Property protected: Confidentiality, Integrity, Availability

Logical Protection

Identification and Authentication

Security Level 2

2060 Password protection with individual passwords. It should not be possible to bypass the password protection; for example, by booting from another medium or by interrupting the boot process. It is recommended that the passwords meet the recommendations for passwords described in Chapter 5.

Property protected: Confidentiality, Integrity, Availability

Access Control

Security Level 2

2070 If the user workstation is holding data on a local disk and is shared among many users, then the data should be protected by individual access control mechanisms.

Property protected: Confidentiality, Integrity, Availability

Security Level 3

2080 If the user workstation is holding company confidential data on a local disk, then the disk should either be removable (and it shall always be removed when the user is not using the system) or the hard disk should be encrypted with strong encryption. Appropriate physical protection of a removed hard disk will be needed.

Property protected: Confidentiality, Integrity, Availability

Organisation and Procedures

Installation and Configuration

Security Level 2

2090 Only standard configurations should be installed, when possible, to simplify system management and to limit the risk of system software conflicts.

Property protected: Integrity, Availability

The report is compared with the current organisation's ICT practices in order to estimate the security awareness in the organisation. This is done by asking the operational staff a set of security questions, which constitute the chosen security policy. Satisfactory answers to the questionnaires indicate security awareness. This could further assist in sorting out from among the presented countermeasures which ones are being practised by the organisation and which are not.

2.5 Fourth step – Survey Report

The results of comparisons in step three (3) are the security benchmarking documented in a survey report that gives an overview of security awareness and the 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. The outcome report can also be used to suggest increased security measures. It is emphasised in BRITS that these ICT security measures should be cost effective since there is no reason for spending resources on technical measures other than a clear link to safeguard the organisation's mission.

2.6 Fifth step – Management Review

During this stage, the mitigation plan is priced and presented to the management for review. The security policy and the suggested increased security measures agreed on will then be reflected in the proposed mitigation plan price.

2.7 Sixth step – Management decision

At this stage, top management have to decide if the damage exposures inherent in the organisation's service should be financially hedged or not. It is during this stage that management must also decide if security should be increased in the information systems that produce the organisation's services to support the organisation's core objectives. If accepted by the management the next stage to consider is full implementation. At the very least, the security awareness achieved in the survey report should be fulfilled in order to have valid countermeasures and consequently to safeguard the organisation's mission.

2.8 Seventh step – Implementation and Monitoring

In principle, steps one to six were mainly analytical: the solutions are still "on the drawing board" - the process referred to in Information Security Management Systems (ISMS) [Bjorck, 2001]. The implementation and monitoring stage takes the conceptual level and makes it work in the organisation. This entails, for example, installation and configuration of technical security mechanisms (e.g. user policy, backup plans, etc), as well as information security awareness and training of employees.

3. Discussion

The end goal in the BRITS process is to design and develop countermeasures tailored to the organisation that will remedy the vulnerabilities and deficiencies that have been identified. This can be made possible by applying the EMitL database to generate tailor-made security policies possible for the different hedge policies. These security policies can be used to guide the line management in their day-to-day operations of the ICT. Lastly the cost of the damage exposure inherent in the organisation's service can be estimated in a better way as indicated in steps 4 and 5, and thereby be incorporated into the service price. This process is iterative and the knowledge gained

in one circle can be used to control the implementation and monitoring in another circle. It is expected that if the EML is to be worked out, it should be less value in the second round, etc.

4. Use of BRITIS in our study

In our study the BRITS framework was utilised in five non-commercial organisations, in an attempt to address the ICT security management problem from a senior management perspective. Using data gathered in responses from the top management and operational management, analysis of the same was performed for each organisation. The results are summarised in Table 3, where 4 represents the highest level of potential risk, 3 indicates medium—high, 2 indicates medium, 1 indicates low and 0 (zero) means not applicable. The EMitL tool interface has only one hedge policy security level for each set of damage exposures. Therefore an assumption had to be made where more than one security level is indicated, in order to increase the overall security level. This means one has to consider a higher security level where more than one security level exists. Results from each column were summarised first and then fed into the EMitL tool (See Figure 4 in section 2.2 above). Table 2 shows how the security levels had been assumed to reflect the level that appears with the highest frequency (Assumed Running Levels – ARL).

Table 2 **Damage exposure levels (Security levels)**

	Damage exposure levels (Security level)				
Damage exposures	Organ. **X**	Organ. **Y**	Organ. **Z**	Organ. **U**	Organ. **V**
Liability					
Service Interruption	1	0	0	4	0
Fraud & Embezzlement	0	2	0	2	0
Robbery & Theft	0	0	4	2	0
Defamation	3	2	3	1	2
Infringement of Privacy	2	2	2	2	2
Infringement of trademark,© etc.	2	0	3	0	2
Loss of Property					
Fraud & Embezzlement	1	4	4	3	1
Robbery & Theft	0	0	2	2	0
Service Interruption					
Loss of sales	0	0	0	4	0
Extra expense	3	4	3	4	3

In case the same frequency is observed, a higher security level is assumed in order to increase the level of assurance. In the table, organisation **X** had ARL 2, 1 and 3 respectively as shown also in the interface in Figure 4.

Table 3 **Different input parameters to EmitL database**

Organisation	Liability						A.R.L	L/Property		A.R.L	B/Interrp		A.R.L	Output
	BI	FE	RT	DE	IP	IT		FE	RT		LS	EE		Countermeasures
X	√	×	×	√	√	√	2	√	×	1	×	√	3	847
Y	×	√	×	√	√	×	2	√	×	4	×	√	4	802
Z	×	√	√	√	√	√	3	√	√	3	×	√	3	880
U	√	√	√	√	√	×	2	√	√	3	√	√	4	803
V	×	×	×	√	√	√	2	√	×	1	×	√	3	847

Key:
BI – Business Interruption
FE - Fraud and Embezzlement
RT – Robbery and Theft
DE – Defamation
IP – Infringement of Privacy
IT – Infringement of Trademark
A.R.L – Assumed Running Level (EMitL – database)
× - Not applicable
√ - Applicable

The outcome generated after running the EMitL tool with the supplied parameters from Table 3 is a report consisting of various security countermeasures. The report can be viewed on screen or exported to a Word file and printed. Depending on the parameters supplied for a particular organisation, the length of the generated reports typically ranged from 90 to 108 pages with countermeasures ranging from 802-880 (see last column – Table 3). The output countermeasures consist of logical security measures structured into four security levels (security level 1, 2, 3, and 4). These measures are mapped to IT security properties, confidentiality (C), Availability (A) and Integrity (I) as shown in figures 5 and 6. Some measures protect only one security property (referred to as unique measures), some protect two security properties (referred to as dual measures) and some protect all three security properties (referred to as generic measures).

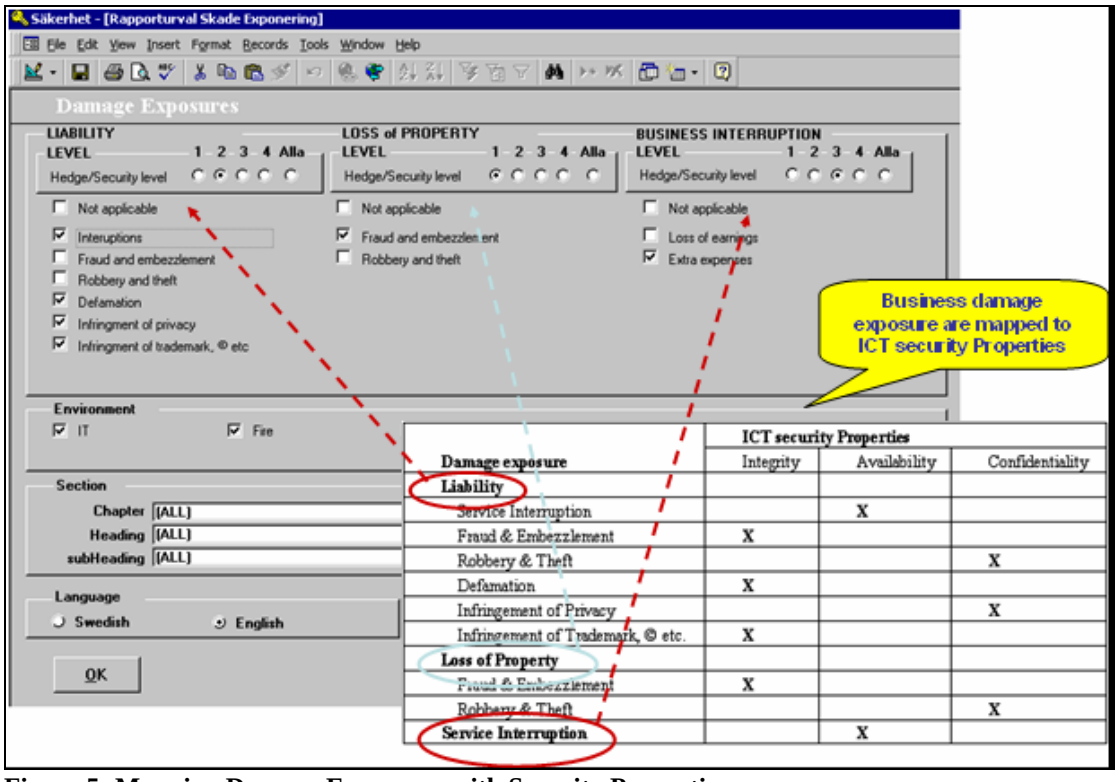


Figure 5: Mapping Damage Exposures with Security Properties

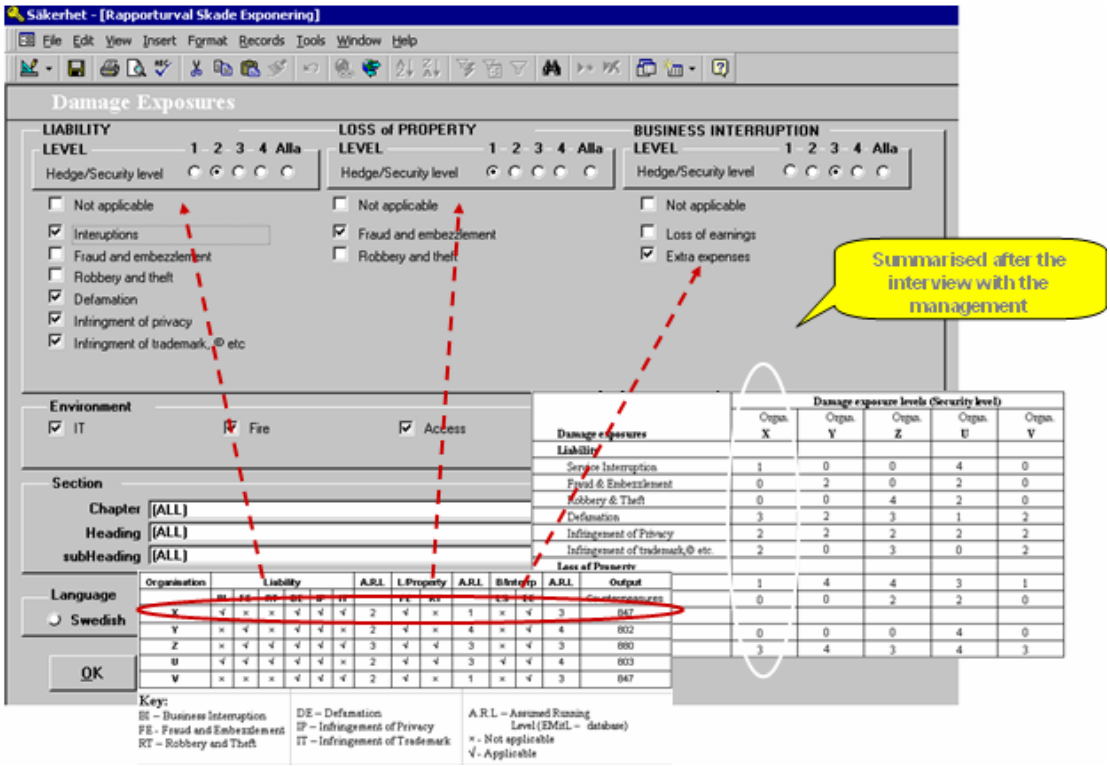


Figure 6: Showing the assumed running levels

An analysis was then made to find out to what extent a given type of security countermeasure addresses the security problem and at what security level.

4. Results

The details and analysis of the results of the case study findings are reported in PAPER II and in (Bakari, 2005).

Appendix H

Appendix H: Case 2 – OCTAVE when applied to Organisation X

1. Introduction

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk-based strategic assessment and planning technique for ICT security. OCTAVE is self directed, meaning that staff from an organisation assume responsibility for setting the organisation's security strategy, by increasing their knowledge of their organisation's security-related practices and processes to capture the current state of security practice within the organisation. Risks to the most critical assets are used to prioritise areas of improvement and set the security strategy for the organisation.

In this brief report we present our experience of applying tailored OCTAVE in organisation X. As pointed out in the main body of the thesis, organisation **X** is a higher learning institute with approximately 1,700 staff (academic and administrative) and a student population of approximately 14,000 (undergraduate and postgraduate). The utilisation of ICT at organisation **X** can be traced back to 1995, when the ICT strategic plan was put in place for the first time. The state of ICT security management can be found in PAPER I.

Despite some deployed technical countermeasures, cases of insecurity were found to be on the increase in the organisation. For example, the number of reported cases of virus attacks in the various information systems leading to unavailability of critical information was on the increase, resulting in confidentiality and integrity problems. There were several cases of viruses and worm infestations in the organisation's network as well as e-mail attachments. There were also cases of important data being deleted without any back-up, and computers with critical information crashing. Other problems stem from users being unaware of simple security precautions like not opening an attachment from a suspicious e-mail. Others are from technical staff disrupting normal operations in the network through mistakes in system configurations. There was therefore a need to address this problem.

It was in response to addressing this requirement that the workshop which involved the full spectrum of management - senior management, operational area management, professional service staff and ICT professionals - was organised.

2. Methodology

We followed the OCTAVE methodology as detailed in OCTAVE, tailored to suit organisation X as follows. First we took advantage of the results of the main research work, in particular the state of ICT security management as reported in PAPER I and by Bakari (2005), in addition to the observed increase in reported security incidents in the organisation as highlighted in the preceding section. In other words, we used the results from study 1 and these observations to ague for the need to apply the OCTAVE methodology to assess the ICT security problem in the organisation and suggest ways to address the problem. We used the following OCTAVE features to prepare and run a workshop:

(a) Identify potential participants (senior, operational, service operations, and IT staff) from the organisational structure.
(b) Identify in each group a potential facilitator and a person who can take notes during the discussion as proposed in the OCTAVE process.
(c) During the workshop, different management levels of an organisation work together to identify critical ICT assets, the security risk to those assets, and then gather some ideas on what to do about those risks
(d) Staff from various sectors of the organisation brought their experience and knowledge, which was pitched against a set of recognised ICT security standards. By doing this, it was possible to determine where organisation X's weaknesses are (vulnerabilities). From their knowledge and job experience, they were able to identify the critical ICT assets, their security requirements and what protection is required.
(e) The approach enables the collection of ICT security data, which can be used at later stages to develop threat profiles for the critical ICT assets, identify the ICT security risks and develop protection strategies.

In the following section we discuss how we organised the workshop.

3. The Workshop

We managed to organise a one-day workshop which took place in a venue which was allocated about 15Km from where the organisation is situated and from the city. The idea here was to get the full participation of the participants. The workshop took place on 11th October, 2005 as detailed in tables 1 and 2. We had full support from the management financially as well as their presence in the workshop. For example, the welcome and opening remarks were given by the senior management, focusing on the need for and importance of the workshop. The participation was as summarised in the table below.

Table 1: Workshop Participants

No.	Participants' Group	Who they were in particular	Total
1.	Senior Management	Chief Academic Officer, Chief Administrative officer, Directors from various major departments	8
2	Operational Managers	Heads of major units such as Information management unit, Finance, Legal, Examination	11
3	Professional Service Staff	Heads or senior staff of sections such as Examinations, payroll, student admission	9
4	IT staff	System administrators from the faculties and major units	8
	Total		**36**

3.1 Facilitation

One week before the workshop we had sessions with the facilitators of different groups on how to facilitate the individual sessions during the workshop. We used customised worksheets to elicit knowledge from each group as suggested in the OCTAVE processes.

Each participant was involved in one of the group discussions. Each group had a facilitator, who guided the group to elicit the required data. In some cases, the facilitator wrote on a screen or flipchart, and in others a specific person was appointed to do that for the group and given some orientation on how to do it.

During the first phase (see table 2), the groups were guided to:

(a) Identify critical ICT assets and prioritise them
(b) Identify the security requirements of the ICT assets identified
(c) Identify areas of ICT security concern in the organisation
(d) Identify the current protection strategies
(e) Identify the current organisational vulnerabilities

During the second phase, the groups reassembled and continued where they left off. In some groups they had to review what they had gathered to see if there were any additions or modifications needed.

After the two main sessions, we conducted a brief presentation on tentative protection strategies. This was then followed by a round-table discussion when participants had the opportunity to give their views on what could be done to address the security problem.

Finally, workshop proceedings detailing all the issues raised in the discussion were prepared and submitted to the organisation's IT unit for further action.

4. Lessons learned

(i) The OCTAVE process was very useful in that each step is very detailed and what we did was just to customise the steps to suite our requirements. For example, we spent time in the workshop to give an overview of the problem to the participants, although most of them were the ones involved in the study 1 survey and so they had some idea of the information requested in the worksheet for discussion. We also found that the champion and facilitators need to understand and master the OCTAVE processes before the workshop. Our experience is that this also helps in the process of customisation of the worksheet. In short, the process requires that at least the champion should be an expert in the area of ICT risk management and the OCTAVE processes in particular.

(ii) The support from the management is very important for the success of the workshop and hence the OCTAVE process. Although we had some problems getting their full participation during the workshop, their commitment made other staff take the workshop seriously.

(iii) Everybody in the entire proposed group confirmed that he or she would participate in person. But surprisingly, on the day of the workshop we had a number of instances where some potential participants apologised for not attending and instead they sent their representatives who were mostly technical people. We coped with this problem by reshuffling some of the

group members, depending on their knowledge, to an appropriate group before we started the session. Somehow this affected the purpose of the workshop.

(iv) The workshop process itself created a very big impact on ICT security in the organisation. In other words, the workshop also acted as an intensive awareness session.

Table 2: ICT security Workshop Timetable – Beachcomber Hotel & Resort, Dar es Salaam, Tanzania, October 11th 2005

No.	Event	Detail	Time	Responsible
	Arrival		8:30 – 8:45	
	Registration		8:45 – 9:00	Registration
		Session One		
	Welcome			Senior management
	Opening Remarks		9:00 – 9:05	Senior management
	Briefing	The General ICT Security status of the organisation	9:05 – 9:15	
	Presentation	Basics of ICT Security and summary of initial findings from ICT security survey in the Organisation	9:15 -10:15	Researcher (J. K. Bakari)
	Presentation	Main workshop objectives and methodology (OCTAVE)	10:15 – 10:35	Research Assistant (Master student – D. Fuli)
		Tea break 10:35 – 10:55		
		Session Two		
	Group discussions Phase One	Senior management group	10:55 -1:15	Facilitator & Senior Management
		Operational area management group	10:55 -1:15	Facilitator & Operational management
		Service Operations staff group	10:55 -1:15	Facilitator & Service operations staff
		IT staff group	10:55 -1:15	Facilitator & IT staff
		Lunch 1:15 – 2:15		
		Session Three		
	Group discussions Phase Two	Senior management group	2:15 – 3:15	Facilitator & Senior Management
		Operational area management group	2:15 – 3:15	Facilitator & Operational management
		Service Operations staff group	2:15 – 3:15	Facilitator & Service operations staff
		IT staff group	2:15 – 3:15	Facilitator & IT staff
		Tea Break 3:15 – 3:35		
	Presentation	Establishing tentative protection strategies	3:35 – 3:45	Researcher (J. K. Bakari)
	General Discussion	Establish tentative protection strategies	3:45 – 4:40	All
	Closing Remarks		4:40	Facilitators & Senior Management

DEPARTMENT OF COMPUTER AND SYSTEMS SCIENCES
Stockholm University/KTH
www.dsv.su.se/eng/publikationer/index.html
Ph.D. theses:

No 91-004 **Olsson, Jan**
An Architecture for Diagnostic Reasoning Based on Causal Models
No 93-008 **Orci, Terttu**
Temporal Reasoning and Data Bases
No 93-009 **Eriksson, Lars-Henrik**
Finitary Partial Definitions and General Logic
No 93-010 **Johannesson, Paul**
Schema Integration Schema Translation, and Interoperability in Federated Information Systems
No 93-018 **Wangler, Benkt**
Contributions to Functional Requirements Modelling
No 93-019 **Boman, Magnus**
A Logical Specification for Federated Information Systems
No 93-024 **Rayner, Manny**
Abductive Equivalential Translation and its Application to Natural-Language Database Interfacing
No 93-025 **Idestam-Almquist, Peter**
Generalization of Clauses
No 93-026 **Aronsson, Martin**
GCLA: The Design, Use, and Implementation of a Program Development
No 93-029 **Boström, Henrik**
Explanation-Based Transformation of Logic programs
No 94-001 **Samuelsson, Christer**
Fast Natural Language Parsing Using Explanation-Based Learning
No 94-003 **Ekenberg, Love**
Decision Support in Numerically Imprecise Domains
No 94-004 **Kowalski, Stewart**
IT Insecurity: A Multi-disciplinary Inquiry
No 94-007 **Asker, Lars**
Partial Explanations as a Basis for Learning
No 94-009 **Kjellin, Harald**
A Method for Acquiring and Refining Knowledge in Weak Theory Domains
No 94-011 **Britts, Stefan**
Object Database Design
No 94-014 **Kilander, Fredrik**
Incremental Conceptual Clustering in an On-Line Application
No 95-019 **Song, Wei**
Schema Integration: - Principles, Methods and Applications
No 95-050 **Johansson, Anna-Lena**
Logic Program Synthesis Using Schema Instantiation in an Interactive Environment
No 95-054 **Stensmo, Magnus**
Adaptive Automated Diagnosis
No 96-004 **Wærn, Annika**
Recognising Human Plans: Issues for Plan Recognition in Human - Computer Interaction
No 96-006 **Orsvärn, Klas**
Knowledge Modelling with Libraries of Task Decomposition Methods
No 96-008 **Dalianis, Hercules**
Concise Natural Language Generation from Formal Specifications
No 96-009 **Holm, Peter**
On the Design and Usage of Information Technology and the Structuring of Communication and Work
No 96-018 **Höök, Kristina**
A Glass Box Approach to Adaptive Hypermedia
No 96-021 **Yngström, Louise**
A Systemic-Holistic Approach to Academic Programmes in IT Security

No 97-005 **Wohed, Rolf**
A Language for Enterprise and Information System Modelling
No 97-008 **Gambäck, Björn**
Processing Swedish Sentences: A Unification-Based Grammar and Some Applications
No 97-010 **Kapidzic Cicovic, Nada**
Extended Certificate Management System: Design and Protocols
No 97-011 **Danielson, Mats**
Computational Decision Analysis
No 97-012 **Wijkman, Pierre**
Contributions to Evolutionary Computation
No 97-017 **Zhang, Ying**
Multi-Temporal Database Management with a Visual Query Interface
No 98-001 **Essler, Ulf**
Analyzing Groupware Adoption: A Framework and Three Case Studies in Lotus Notes Deployment
No 98-008 **Koistinen, Jari**
Contributions in Distributed Object Systems Engineering
No 99-009 **Hakkarainen, Sari**
Dynamic Aspects and Semantic Enrichment in Schema Comparison
No 99-015 **Magnusson, Christer**
Hedging Shareholder Value in an IT dependent Business society - the Framework BRITS
No 00-004 **Verhagen, Henricus**
Norm Autonomous Agents
No 00-006 **Wohed, Petia**
Schema Quality, Schema Enrichment, and Reuse in Information Systems Analysis
No 01-001 **Hökenhammar, Peter**
Integrerad Beställningsprocess vid Datasystemutveckling
No 01-008 **von Schéele, Fabian**
Controlling Time and Communication in Service Economy
No 01-015 **Kajko-Mattsson, Mira**
Corrective Maintenance Maturity Model: Problem Management
No 01-019 **Stirna, Janis**
The Influence of Intentional and Situational Factors on Enterprise Modelling Tool Acquisition in Organisations
No 01-020 **Persson, Anne**
Enterprise Modelling in Practice: Situational Factors and their Influence on Adopting a Participative Approach
No 02-003 **Sneiders, Eriks**
Automated Question Answering: Template-Based Approach
No 02-005 **Eineborg, Martin**
Inductive Logic Programming for Part-of-Speech Tagging
No 02-006 **Bider, Ilia**
State-Oriented Business Process Modelling: Principles, Theory and Practice
No 02-007 **Malmberg, Åke**
Notations Supporting Knowledge Acquisition from Multiple Sources
No 02-012 **Männikkö-Barbutiu, Sirkku**
SENIOR CYBORGS- About Appropriation of Personal Computers Among Some Swedish Elderly People
No 02-028 **Brash, Danny**
Reuse in Information Systems Development: A Qualitative Inquiry
No 03-001 **Svensson, Martin**
Designing, Defining and Evaluating Social Navigation
No 03-002 **Espinoza, Fredrik**
Individual Service Provisioning
No 03-004 **Eriksson-Granskog, Agneta**
General Metarules for Interactive Modular Construction of Natural Deduction Proofs
No 03-005 **De Zoysa, T. Nandika Kasun**
A Model of Security Architecture for Multi-Party Transactions
No 03-008 **Tholander, Jakob**
Constructing to Learn, Learning to Construct - Studies on Computational Tools for Learning

No 03-009 **Karlgren, Klas**
Mastering the Use of Gobbledygook - Studies on the Development of Expertise Through Exposure to Experienced Practitioners' Deliberation on Authentic Problems
No 03-014 **Kjellman, Arne**
Constructive Systems Science - The Only Remaining Alternative?
No 03-015 **Rydberg Fåhræus, Eva**
A Triple Helix of Learning Processes - How to cultivate learning, communication and collaboration among distance-education learners
No 03-016 **Zemke, Stefan**
Data Mining for Prediction - Financial Series Case
No 04-002 **Hulth, Anette**
Combining Machine Learning and Natural Language Processing for Automatic Keyword Extraction
No 04-011 **Jayaweera, Prasad M**.
A Unified Framework for e-Commerce Systems Development: *Business Process Patterns Perspective*
No 04-013 **Söderström, Eva**
B2B Standards Implementation: Issues and Solutions
No 04-014 **Backlund, Per**
Development Process Knowledge Transfer through Method Adaptation, Implementation, and Use
No 05-003 **Davies, Guy**
Mapping and Integration of Schema Representations of Component Specifications
No 05-004 **Jansson, Eva**
Working Together when Being Apart – An Analysis of Distributed Collaborative Work through ICT from an Organizational and Psychosocial Perspective
No 05-007 **Cöster, Rickard**
Algorithms and Representations for Personalised Information Access
No 05-009 **Ciobanu Morogan, Matei**
Security System for Ad-hoc Wireless Networks based on Generic Secure Objects
No 05-010 **Björck, Fredrik**
Discovering Information Security Management
No 05-012 **Brouwers, Lisa**
Microsimulation Models for Disaster Policy Making
No 05-014 **Näckros, Kjell**
Visualising Security through Computer Games
Investigating Game-Based Instruction in ICT Security: an Experimental approach
No 05-015 **Bylund, Markus**
A Design Rationale for Pervasive Computing
No 05-016 **Strand, Mattias**
External Data Incorporation into Data Warehouses
No 05-020 **Casmir, Respickius**
A Dynamic and Adaptive Information Security Awareness (DAISA) approach
No 05-021 **Svensson, Harald**
Developing Support for Agile and Plan-Driven Methods
No 05-022 **Rudström, Åsa**
Co-Construction of Hybrid Spaces
No 06-005 **Lindgren, Tony**
Methods of Solving Conflicts among Induced Rules
No 06-009 **Wrigstad, Tobias**
Owner-Based Alias Management
No 06-011 **Skoglund, Mats**
Curbing Dependencies in Software Evolution
No 06-012 **Zdravkovic, Jelena**
Process Integration for the Extended Enterprise
No 06-013 **Olsson Neve, Theresia**
Capturing and Analysing Emotions to Support Organisational Learning:
The Affect Based Learning Matrix
No 06-016 **Chaula, Job Asheri**
A Socio-Technical Analysis of Information Systems Security Assurance
A Case Study for Effective Assurance

No 06-017 **Tarimo, Charles N.**
ICT Security Readiness Checklist for Developing Countries:
A Social-Technical Approach
No 06-020 **Kifle Gelan, Mengistu**
A Theoretical Model for Telemedicine
- Social and Value Outcomes in Sub-Saharan Africa
No 07-001 **Fernaeus, Ylva**
Let's Make a Digital Patchwork
Designing for Children's Creative Play with Programming Materials