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

A Dynamic and Adaptive Information Security Awareness (DAISA) Approach

Respickius Casmir

December 2005

Submitted to Stockholm University in partial fulfilment of the requirements for the degree of Doctor of Philosophy
"If you teach a person what to learn, you are preparing that person for the past. If you teach a person how to learn, you are preparing that person for the future"

--Cyril Orvin Houle

Respickius Casmir
A Dynamic and Adaptive Information Security Awareness (DAISA) Approach
Department of Computer and Systems Sciences
Stockholm University/Royal Institute of Technology
Report Series
No. 05-020
ISBN 91-7155-154-9
ISSN 1101-8526
ISRN SU-KTH/DSV/R--05/20--SE

Printed by
Universitetsservice US-AB, Stockholm, Sweden, 2005

©Respickius Casmir 2005
Abstract

Information systems fail not only because of problems with technology used and technical incompetence of professionals administering them but also because of lack of security awareness to the end users. In addition, various research results have revealed that security and reliability of IS/IT systems is a function of technology, processes and people. This research has focused on the latter aiming at developing an integrated information security education, training and awareness learning continuum. Particularly, the research has focused on developing countries where a little has been done to address information security learning continuum. The research has been done in two cyclic phases in which cycle one has chiefly addressed security education and training aspects whereas cycle two has mainly focused on security awareness aspects. Based on empirical analysis of security practices in organisations, the thesis proposes a Dynamic and Adaptive Information Security Awareness (DAISA) approach. Founded on six interdependent pillars, the approach delineates high level guidelines for establishing and maintaining information security awareness programs at workplaces.
Acknowledgements

A research journey is easier when you travel together. Interdependency is certainly more valuable than independency. This thesis is results of a four-year challenging work during which I have been supported by many people. It is my pleasure that I take this opportunity to express my gratitude to them all.

I would like to thank my supervisor Prof. Louise Yngström whose guidance, support, critique and encouragement helped me a lot at all times of the research. Thanks to Prof. Beda Mutagahywa for his valuable advice and encouragement in the course of this work.

Thanks to my friend Norbert Nongwa for helping me with tiresome tasks of distribution and collection of questionnaires. My appreciations to all my friends and colleagues in particular Jeffy Mwakalinga, Fredrik Björck and Charles Tarimo with whom I had many valuable discussions on the area of IT security. Thanks to Fatima Santala, Rodolfo Candia, Birgitta Olsson, Niklas Brunbäck and Sven Olofsson, for assisting me on logistical and technical matters respectively.

My gratitude goes to the Swedish International Development Agency (SIDA) for funding my research. I would like to extend my thanks to all personnel at the Department of Computer and Systems Sciences (DSV) of Stockholm University and Royal Institute of Technology for their support and cooperation in the course of my study. I wish to thank the University of Dar es Salaam for granting me an opportunity to pursue my PhD studies.

I am very grateful to my wife, Neema, for her love and patience during the study period. One of the best experiences that we lived through in this period was the birth of our son, Victor, who provided an additional and joyful dimension to our life mission.
To my wife, Neema, and my son, Victor
# TABLE OF CONTENTS

## INTRODUCTION ................................................................................................................................. 1

1.1 Background ................................................................................................................................. 2
1.2 Motivation for the Research ....................................................................................................... 6
1.3 Research Question ...................................................................................................................... 6
1.4 Purpose of the Research ............................................................................................................ 8
1.5 Research Methodology .............................................................................................................. 9
1.6 Overview of the Research Process ............................................................................................ 14
1.7 Theoretical Foundation of the Research ................................................................................ 16
1.8 Limitations and Assumptions ................................................................................................. 21
1.9 Contributions .......................................................................................................................... 22
1.10 Thesis Layout ......................................................................................................................... 25

## INFORMATION SECURITY IN A BIGGER PICTURE ........................................................................ 27

2.1 A Conceptual IT System .............................................................................................................. 27
2.2 Information Assets .................................................................................................................... 34
2.3 Defining Information Security .................................................................................................. 35
2.4 Security Risks, Threats and Vulnerabilities ............................................................................ 39
2.5 Security Perspectives .............................................................................................................. 45
2.6 Security Countermeasures ....................................................................................................... 48
2.7 Security Evaluation Criteria and Security Metrics .................................................................. 50
2.8 Information Security Learning Continuum ............................................................................. 56
2.8 Chapter Summary .................................................................................................................... 57

## DETAILED RESEARCH PROCESS ................................................................................................. 59

3.1 Phase One ............................................................................................................................... 59
3.2 Key Findings in Phase One ...................................................................................................... 64
3.3 Output of Phase One ................................................................................................................. 65
3.4 Phase Two ............................................................................................................................. 68
3.5 Evaluation of Phase One ......................................................................................................... 69
3.6 Key Findings from Evaluation of Phase One .......................................................................... 84
3.7 Other Research Activities in Phase Two ................................................................................ 84
3.8 Key Findings in Phase Two ..................................................................................................... 87
3.9 Output of Phase Two .............................................................................................................. 88
3.10 Impact of the Research Activities ......................................................................................... 90
3.11 Chapter Summary .................................................................................................................. 93

## EMPIRICAL ANALYSIS OF SECURITY SURVEY ........................................................................ 95

4.1 Purpose of the Security Survey ............................................................................................... 95
4.2 Questionnaire Design and Management ............................................................................... 97
4.3 Sampling Techniques Used .................................................................................................... 100
4.4 Analysis of Questionnaires .................................................................................................... 102
4.5 Discussion and Interpretation of the Results ........................................................................ 102
4.7 Reflections from the Questionnaires Results ........................................................................ 126
4.8 Chapter Summary .................................................................................................................. 133

## RELATED PUBLICATIONS .......................................................................................................... 135

5.1 Summaries of Refereed Papers ............................................................................................... 135
5.2 Summaries of Newsletter Articles .......................................................................................... 147
# Table of Contents

5.3 Reflections from the Papers and Newsletter Articles ........................................... 152  
5.4 Chapter Summary ................................................................................................. 152  

**THE DYNAMIC AND ADAPTIVE INFORMATION SECURITY AWARENESS (DAISA) APPROACH** ................................................................................................................. 153  

6.1 Overview of the DAISA Approach ........................................................................ 153  
6.2 Key Elements of the DAISA Approach ................................................................ 156  
6.3 Getting Started ..................................................................................................... 165  
6.4 Security Awareness Metrics .................................................................................. 167  
6.5 Implementation Strategy for the DAISA Approach .............................................. 169  
6.6 Keeping Pace with Changing Cyber Threats and Vulnerabilities ....................... 172  
6.7 Security Awareness as Part of Organisational Culture ...................................... 172  
6.8 Validation of the DAISA Approach ..................................................................... 174  
6.9 Chapter Summary ................................................................................................. 179  

**CONCLUSIONS** ..................................................................................................... 181  

7.1 Validation of the Research ................................................................................... 181  
7.2 Summary of Research Contributions .................................................................. 187  
7.3 Conclusions ......................................................................................................... 191  
7.4 Suggestions for Further Work ............................................................................ 192  

**REFERENCES** ....................................................................................................... 193  

**APPENDICES** ....................................................................................................... 203  

Appendix A: Questionnaire for Evaluation of a Short Course .................................... 204  
Appendix B: Pre-Training Assessment Questionnaire .............................................. 205  
Appendix C: Post-Training Assessment Questionnaire ............................................ 206  
Appendix D: Questionnaire for Evaluation of Information Security Practices ........... 207
Chapter 1

INTRODUCTION

Information systems fail not only because of problems with technology used and technical incompetence of professionals administering them but also because of lack of security awareness to the end users. Reliability and security of Information Technology (IT) systems is thus a function of Technology, Processes, and People Schneier (2000); Anderson (2001). This research primarily focuses on the latter, specifically on creating and maintaining information security awareness to the end users. According to DTI (2004) the United Kingdom Department of Trade and Industry (DTI):

“A well-trained, well-informed workforce is one of the most powerful weapons in an information security manager’s arsenal.”

.....DTI (UK)

Furthering the DTI’s assertion, we argue that technology in itself does not work unless people make it work. This argument is based on the fact that people design, implement, manage and use technology. Conversely, it is people who misuse technology. The misuse of or security breach to IT systems might be intentional, accidental or out of mere ignorance. According to Pfleeger (1997) in either case outcomes are always loss of confidentiality, integrity, or availability of information stored, processed or transmitted within
IT systems. In the light of the above, this thesis proposes a Dynamic and Adaptive Information Security Awareness (DAISA) approach to enhance security in organisations, particularly, in developing countries. The proposed DAISA approach is meant to complement the previously developed IT security curricula Casmir (2003) with a view of fulfilling the overall purpose of the research discussed later in this chapter.

In this chapter we give an overview of the research including the background to and motivation for the research, purpose of the research, research question, methodology used, contributions, and scope of the thesis. The chapter finally gives an outline and structure of the thesis.

1.1 Background

Perhaps it is worth to point out that this work was specifically done in Tanzania as a case study. The ultimate goal was to investigate how information security issues were being addressed in developing countries. There are at least three reasons that influenced the choice of Tanzania as our case study for this research. First, is its unique history when it comes to deployment of computers and other IT systems in the country Lamtrac (2001); Esselaar (2001). Tanzania was late to embark on Information and Communication Technology (ICT). This was partly due to strict policies on importing computers to the country Lamtrac (2001) from 1974 to early 90’s. Before 1994 there were no Internet; no mobile phone; no Automated Teller Machine (ATM) services; and no Television station in Tanzania. The latter was only present and accessible in Zanzibar which covers about 2.9% of the
entire population of nearly 34 million people. A nearly 20-year restriction on import of computers had adversely impacted the country’s development in terms of ICT skills. As a result of this ICT dormant era, there was neither a policy in place to address ICT issues in the country.

However, the pace with which ICT deployment is currently (i.e. in year 2005) moving is relatively high. As Accenture (2001) has put it, Tanzania hopes to illustrate that starting off on the right foot is a key to leapfrogging or “antelope-jumping” many stages of ICT development. Tanzania’s development Vision 2025 (2001) singles out ICT as a key driver for transformation to realise competence and competitiveness. Specifically, the Vision states that, “ICTs are major driving forces for the realisation of the Vision”. In March 2003 Tanzania released the first version of its ICT policy, ICTPolicy (2003), as part of implementations of the Vision 2025. The policy outlines the high level guidelines for ICT development and deployment in the country. Second, we had to narrow down our domain of research since it was not realistic to carry out the study in all developing countries. Since Tanzania is one of the developing countries she, therefore, qualifies as a case study. Third, it was economically feasible and cost effective to carry out this research work in Tanzania since the author comes from there.

Other developments include waiving off of the import duty on computers and computer accessories. This was publicly announced in year 2001 by the Tanzania Government and has been in effect since then to the time of writing this thesis. The move was deliberately meant to encourage as many people as possible to buy computers at affordable prices. Thanks to the Government of
Tanzania for the initiative. Also, the proliferation of Internet cafes in Tanzania was very high, particularly in Dar es Salaam, compared to other Southern African Development Community (SADC) countries Esselaar (2001). In year 2001 the number of Internet cafes was estimated to 1000 Esselaar (2001). The bulk of clients in most of the cafes were teenagers and business people. E-mail services were the most popular activities in the Internet cafes followed by general web surfing. While a number of people were going to the cafes to make telephone calls abroad, which was cheaper via the net, others were going to the cafes on e-business missions. However, the proportion of the latter was relatively small.

Computerization processes were (and still in 2005) at the infancy stages in both public and private sectors in Tanzania. People were enthusiastic and excited to learn on how to use IT facilities especially the Internet. For the majority information security was even not known, and therefore, not a priority at the moment. What mattered most to them was to gain the necessary skills on how to use ICT facilities.

Commencement of this work can be traced back to year 2001 when we organized the first IT security awareness seminar for IT practitioners in Dar es Salaam, Tanzania. At this time we did not have clear picture of what was on the ground as far as IT security is concerned in developing countries such as Tanzania. Precisely, there was apparently nothing published or at least not known to the author with respect to information security handling in Tanzania. Since then we continued with a series of related research activities details of which are presented in Chapters 3, 4, and 5. Findings obtained at every stage
were published in International Conferences and Journal (see Chapter 5 Related Publications).

1.1.1 Uniqueness of Developing Countries

Perhaps one would like to know what is so unique with developing countries in such a way that this research is specifically focusing on them. Here is our response to this query. In developing countries, conditions, constraints, resources and even cultures differ quite significantly from developed countries. This is equally true for economic development and technological advancement. Developed nations are far ahead of developing ones in terms of IT advancement, deployment and utilisation. Terminologies such as ‘The Digital Divide’ have emerged because of these differences. The reasons to this situation, however, are beyond the scope of this thesis. Computerisation processes currently going on are at infancy stages, therefore, we believe this is the right time to introduce security awareness along with computerisations; else we may run the risks of paying higher prices later. This is mainly because in today’s networked world threats and vulnerabilities to information assets are global. On the other hand, some of the things that were considered normal in developed countries; they were ‘new’ in developing countries where the deployment and use of IT systems were at infancy stages. For example while the use of Automated Teller Machines (ATM) is a common thing in developed countries; it is something very new in Tanzania. The use of Internet banking was common in developed countries but even not yet introduced in Tanzania.
1.2 Motivation for the Research

Certainly there are very strong motivations behind this research. Increased deployment and use of computers and other IT systems in Tanzania Esselaar (2001); Accenture (2001); unavailability of publicly known plans and procedures for securing these systems including information security education, training and awareness in the country; and ever increasing cyber threats and risks around world Schneier (2000); Gordon and Ford (2002) motivated the author to carry out this work. While all ICT developments described in section 1.1 were commendable, we argue that its sustainability is at stake should deliberate and appropriate security awareness measures not taken timely. Unfortunately an attacker or a cyber criminal may not wait until people in developing countries become conversant with the use of IT facilities first. In fact, security unawareness of people in this region might be good news to the attackers. They will be happy to capitalise on any available window of vulnerability to compromise IT systems. In this regard the author being a dedicated information security specialist cannot wait until a word is spread to the community of attackers that developing countries are vulnerable.

1.3 Research Question

In its simplest terms, the drive to carry out this research work can be reduced to a single research question as follows:

Which approach can be employed to effectively bring up security awareness, training, and education to IT Systems’ users in developing countries’ environments?
One simple and quick answer one of my colleagues gave to this question was that “just train people in security matters”. However, this answer raised many more questions that were not thought of before, making the issue even more complex than expected. Typical questions that arose include the following:

1) How to start?
2) Where to start?
3) When to start?
4) What about effectiveness of the approach?
5) What about outreach?
6) What about cultural, social and ethical aspects considerations?
7) Are all computer users at the same level of abstraction?
8) Training versus Education dilemma?
9) Security Awareness Program?
10) Security Professional Training?
11) May be all of these?
12) What about kids and teenagers?
13) What is the scope then?

With this endless list of unanswered questions, we could not easily find a ‘silver bullet’ solution to all of them. In an attempt to address the overall research question we investigate it from three different perspectives namely security education, training and awareness. The reason for investigating the three aspects was not only that they were equally important but also that they were interdependent. Taken together they form a ‘lifelong security learning
continuum’. Addressing one at the expense of the other would create a ‘terrible gap’ within the security learning continuum, hence subject the entire continuum at stake. Figure 1.1 depicts the three facets of the information security learning continuum. Detailed discussions on the three facets are presented in Chapter 2. In the process we considered several options out of which the dynamic and adaptive information security awareness (DAISA) approach emerged as the most effective alternative for the purpose at hand. Discussed in Chapter 6, the DAISA approach was meant to complement our initial work that resulted in the IT security curricula Casmir (2003). Excerpt of the initial work is presented and discussed in Chapter 3. The keyword ‘effective’ in our research question is purposely meant to allow for equifinality.

![Figure 1.1: The Three Facets of Information Security Learning Continuum](image)

1.4 Purpose of the Research
The primary purpose of this research was to investigate and propose an effective integrated information security education, training and awareness
learning continuum for IT users in developing countries. To propose an approach that would effectively address the security learning continuum and appropriately respond to most, if not all, of questions raised in section 1.3 above; and eventually, appropriately respond to the main research question.

1.5 Research Methodology

We commenced our research open-mindedly. Our aim was to learn about the current situation in Tanzania in terms of IT security knowledge and practices. Given the nature of the problem and the environment we were conducting our research in; we opted for an action research methodology Grundy (1988); Kemmis and McTaggart (1990); McCutcheon and Jung (1990); Stringer (1999); Carson and Sumara (1997). Despite the many definitions of action research by various authors, this thesis applies the one by McCutcheon and Jung (1990). According to McCutcheon and Jung (1990, pp. 148) action research is defined as a “systemic inquiry that is collective, collaborative, self-reflective, critical and undertaken by participants in the inquiry”. The choice of the methodology was made after going through other various research methodologies Allen-Meares and Lance (1990); Berg (1995). The problem was partly known (i.e. IT security education and awareness) but the environment was new (i.e. a developing country). Therefore, to be able to investigate the research problem there need to be some reality to observe. In the process the researcher may also observe or learn about further magnitude of the problem.
According to Stringer (1999) action research works through three basic steps namely Look, Think and Act. The three steps are described as follows:

**Look** – building a picture and gathering information. When evaluating a particular research situation, we need to define and describe the problem to be investigated and the context in which it is set. We also need to describe what all the participants in the research process (in our case including students, focus group members, and seminar participants) have been doing.

**Think** – interpreting and explaining. When evaluating we analyse and interpret the situation at hand. We reflect on what participants have been doing. We look at areas of success and any deficiencies, issues or problems.

**Act** – resolving issues and problems. In evaluation we judge the worthiness, effectiveness, appropriateness, and outcomes of those activities. We then act to formulate solutions to any problems we are dealing with (Stringer 1999, pp. 18; 43-44; 160).

In this case, the research is both quantitative and qualitative. We designed, distributed, collected and evaluated questionnaires as described in Chapters 3 and 4. We also partly followed the action learning cycle guidelines as specified by the Centre for Applied Research in Education (CARE), University of East Anglia CARE (2001). Figure 1.2 illustrates CARE’s action learning model. With this model learning goes through a four-step cycle as follows:
1) **Act** - Conduct an activity, have an experience (e.g. go on the field trips, implement a plan for activities such as seminars and workshops).

2) **Observe** - How did it go, what did I feel, see, hear, what did I learn from this experience? (e.g. ask the questions above at the end of each session, activity and at the debriefing of the activities workshop).

3) **Reflect/ generalise/ conclude** – Questions like what are the generalizations that could be made from our reflections, are there anything that can be used in the future? Whether there are any ‘rules of thumb’; what conclusions can we draw? (e.g. after reflecting as an individual and with the group what is the learning that can be carried forward into future planned action).

4) **Plan** - Introduce and plan the use of any learning, conclusions, generalisations or “rules of thumb” in the next stage of the activity or

---

**Figure 1.2: The Action-Learning Cycle Model** [Source: CARE (2001, www.uea.ac.uk/care/; Accessed: August 2001)]
other appropriate activity (e.g. the learning are then used in the next phase of work).

We applied the model by conducting 10 IT security awareness seminars to practitioners locally in Tanzania. We also conducted 4 short courses on IT security to undergraduate students from different academic disciplines at the University of Dar es Salaam. Detailed descriptions of seminars and short courses are presented in Chapter 3. In our view, Action Research is a dynamic approach to getting outcomes that gradually adapts to needs Grundy (1988) – even changing needs like security awareness.

Generally, there are three types of action research Masters (1995) namely technical action research; mutual-collaborative action research; and participatory action research. Table 1.1 summarises the descriptions of the generalised three types of action research according to Masters (1995, pp. 7).

<table>
<thead>
<tr>
<th>Philosophical Base</th>
<th>Technical Action Research</th>
<th>Mutual - Collaboration Action Research</th>
<th>Participatory Action Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Sciences</td>
<td>Historical - hermeneutic</td>
<td>Critical Sciences</td>
<td></td>
</tr>
<tr>
<td><strong>The nature of reality</strong></td>
<td>Single, measurable, fragmental</td>
<td>Multiple, constructed, holistic</td>
<td>Social, economic. Exists with problems of equity and hegemony</td>
</tr>
<tr>
<td><strong>Problem</strong></td>
<td>Defined in advance</td>
<td>Defined in situation</td>
<td>Defined in the situation based on values clarification</td>
</tr>
<tr>
<td>Philosophical Base</td>
<td>Technical Action Research</td>
<td>Mutual - Collaboration Action Research</td>
<td>Participatory Action Research</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td>Natural Sciences</td>
<td>Historical - hermeneutic</td>
<td>Critical Sciences</td>
</tr>
<tr>
<td>Relationship between the Knower and Known</td>
<td>Separate</td>
<td>Interrelated, dialogic</td>
<td>Interrelated, embedded in society</td>
</tr>
<tr>
<td>Focus of collaboration theory</td>
<td>Technical validation, refinement, deduction</td>
<td>Mutual understanding, new theory, inductive</td>
<td>Mutual emancipation, validation, refinement, new theory, inductive, deductive</td>
</tr>
<tr>
<td>Type of knowledge produced</td>
<td>Predictive</td>
<td>Descriptive</td>
<td>Predictive, descriptive</td>
</tr>
<tr>
<td>Change duration</td>
<td>Short lived</td>
<td>Longer lasting, dependent on individuals</td>
<td>Social change, emancipation</td>
</tr>
<tr>
<td>The nature of understanding</td>
<td>Events explained in terms of real causes and simultaneous effects</td>
<td>Events are understood through active mental work, interactions with external context, transactions between one’s mental work and external context</td>
<td>Events are understood in terms of social and economic hindrances to true equity</td>
</tr>
<tr>
<td>The role of value in research</td>
<td>Value free</td>
<td>Value bounded</td>
<td>Related to values of equity</td>
</tr>
<tr>
<td>Purpose of research</td>
<td>Discovery of laws underlying reality</td>
<td>Understand what occurs and the meaning people make of phenomena</td>
<td>Uncover and understand what constrains equity and supports hegemony to free oneself of false consciousness and change practice toward more equity</td>
</tr>
</tbody>
</table>
Based on Table 1.1 and as per discussions made in Chapter 3, our research clearly falls under type 2 of action research i.e. Mutual–Collaboration. The research problem we were attempting to address was defined based on the situation on the field; and in collaboration with the stakeholders.

### 1.6 Overview of the Research Process

This research went through a series of processes as described in Figure 1.3. Each step comprised a set of activities to be accomplished prior to switching to the next phase. This section gives an overview of the research process. Details of the research processes are discussed in Chapter 3.

**Figure 1.3: A Step-wise Path in the Research Process**
In the first step of the research process we applied individual experience to formulate the research question. At the time of commencement of this research, the author had worked within the ICT industry in Tanzania for at least five years. In the second stage we investigated the facts on the ground by conducting seminars and short courses on IT security in Tanzania. We also conducted a number of face-to-face interviews with various stakeholders in the field. Use was made of questionnaires to collect useful information for our research. Moreover, we conducted desk research by using related documentations. Then we gathered and consolidated all relevant information obtained followed by development of an academic IT security curricula. Development of the curricula marked the completion of phase 1 of the research.

Although the curricula were apparently supported by many stakeholders including faculty members and students its implementation was yet to take place at the time of this thesis. One main reason was given for delays in its implementation; that certain resources were required to be in place prior to take off of the program. Resources needed include competent instructors, text and reference books, laboratory tools and equipment, just a few to mention all of which were dependent on availability of adequate financial resources. Efforts were being made to seek for funds for implementation of the program. No timelines were set for launching the program though. There was apparently another implicit reason not mentioned though. Perhaps we made a miscalculation on the timings for the curricula to get the right push forward. We underrated the fact that the threshold for security awareness was yet to be reached by many people including some of the decision makers. This was
revealed in course of evaluation of phase 1 of this research and during the interviews with various stakeholders. For further details on this see Chapter 3. Having observed this situation we amended our plans to directly focus on awareness program per se first, hence the DAISA approach.

To obtain relevant information that guided us to propose the DAISA approach we used various data collection techniques. These include questionnaires, interviews, documentation and literature review, observations, focus group, seminars and short courses. We also published the findings obtained during the process in different international conferences and a journal. Comments and suggestions given during presentations at the conferences have been incorporated and form part of the DAISA approach.

1.7 Theoretical Foundation of the Research

This research is firmly founded on the General System Theory Bertalanffy (1968); Ruben et al (1975) and Cybernetics Wiener (1948); Scrivener (2002). Action research which is our methodology is, in fact, an instance of the General System Theory Bertalanffy (1968). System theory or rather systems science argues that no matter how complex the world we experience might be there are always certain organisation in it that can be described by concepts and principles independent from a specific domain Heylighen (2000). Also, that Taschdjian (1975) if those concepts and principles were properly uncovered it would be possible to analyse any type of systems. The systems approach uniquely differs from analytical approaches in that the former accentuates the interactions and connectedness of the different components
that make up a particular system Bertalanffy (1968). Much as the system approach deals with all types of systems, in practice, it focuses on Klir (1972); Taschdjian (1975) complex, adaptive, and self-regulating systems which might be referred to as Cybernetics Scrivener (2002). A model of an organisation’s IT system described in Chapter 2 clearly falls into this category of systems. In the same perspective Louise Yngström (1996) argues that IT security education issues should be viewed and approached holistically using both systemic as well as systematic means.

Concepts and principles used in systems science mostly emanate from a closely related area of Cybernetics Boyd (1980); Bung and Lansky (1978). The term ‘Cybernetics’ was derived from the Greek word Kybernetes – meaning Steersman Heylighen (2000). It was first introduced by a mathematician Wiener (1948) as the science of communication and control in the animal and the machine Taschdjian (1975). The concept was developed further through Shannon’s information theory Shannon (1948) aiming at optimising the transmission of information through communication channels; and the feedback mechanism used in engineering control systems. Figure 1.4 illustrates a system in interaction with its environment.
1.7.1 Systems Thinking in Relation to Our Methodology

An IT system described in Chapter 2 is a typical instance of a general system. IT systems do not exist in a vacuum but rather they coexist with other real-world systems. To be able to deal with security issues properly we, therefore, need to view it as a system that, in practice, takes in desirable and undesirable inputs. It is the role of a security manager to define the system boundaries and implement controls to see to it that only desirable inputs get into the system. In case it happens that some undesirable inputs have entered the system, they should be properly controlled, say in a ‘sandbox mode’, to minimise their effects.

Typically, the input might include staff, customers, competitors, attackers, consultants, suppliers, temporary staff, ex-staff, partners, and other entities. The list includes both desirable and undesirable entities. These inputs interact in various ways with each other and with the surrounding environment. The same system is expected to give as output secure and reliable services to
legitimate entities no matter how complex the interactions within the system and between the subsystems are. To securely handle interactions between and within input components both technical and non-technical measures are equally required. The former include various security mechanisms and architectures Cheswick and Bellovin (1994); Muftic et al (1993) such as firewalls, Cryptographic tools, Intrusion Detection Systems (IDS), Virtual Private Networks (VPN), Antivirus Software, and other security technologies Stallings (2003). Non-technical measures include policies; procedures; awareness programs; physical security; legal; social and ethical measures.

Looking at Figure 1.4 it can be observed that the system is open to the external environment. The characteristic of open systems, such as an IT system, is the fact that they interact with other systems outside themselves. This interaction has two main segments namely Input –that what enters the system from the outside environment; and Output –that what leaves the system to the environment Bertalanffy (1968). The transformation of input into output by the system is referred to as throughput. In order to talk of the inside and the outside of a given system we first need to be able to distinguish between a system and its environment. A system and its environment are separated by a boundary.

IT systems on the other hand are characterised and shaped by the subjectivity of their managers and users; and are diversely situated socially as well as physically. Such aspects are best addressed by adopting a ‘soft’ systems thinking that takes on managers and users of IT systems in research as objects rather than as subjects. In this respect, an ideal information security specialist
must be both an expert on the aspects of the system which she/he is administering and an executive of learning the organisation’s internal workings. It is against this background Yngström (1996) argues that an area like IS/IT security needs to be dealt with both epistemology Lincoln and Guba (1985) (i.e. what we tell, describe, or understand) and ontology (i.e. what we do in practice) adding that the quest of information security education is to use both. Taking all these into account we find that ontological or hard systems security problems are best handled using systematic or analytical approaches. Also those epistemological or soft systems security problems are best addressed using systemic or holistic approach Yngström (1996).

Relating this research to our methodology one can find that the action (Figure 1.2) starts by specifying a problem, lack of security awareness, (epistemology) followed by an action on that problem. Observation here means analysing and/or questioning using theories, models, or other measures (ontology). Reflection means choosing some of the results, that is, learning about the problem. Plan means to act accordingly with respect to what was learnt. It is important to note that it is not the inclusion of people that makes it soft –rather it is the inclusion of problem-orientation that makes it soft. People may decide to treat a specific problem as either soft –systemically (i.e. as a problem) or hard –systematically (i.e. as a reality). Here we argue that this is the real basic problem with almost all IT security related issues: People just want to solve a problem by Yngström (1996) adding a new token, program, mechanism, or other tools instead of analysing first what or where for that matter are the real problems. By using the action learning cycle this is provided.
1.8 Limitations and Assumptions

It is perhaps natural that such a research work cannot go without making some grounded assumptions. This research is no exception. We made a number of assumptions as follows:

a) *Choice of a case study* – As discussed in Section 1.1 we selected Tanzania as our case study for this work. The assumption made here was that Tanzania being an instance of the developing countries possesses many of the key/important attributes that a developing country has when it comes to IT deployment and usage.

b) *ICT status in developing countries* – It was assumed that the majority of developing countries have similar status in terms of ICT advancement.

c) *Information security awareness* – It was assumed that less, if not none, has been done for developing countries with respect to information security education and awareness. This assumption was backed by the fact that up to the time of writing this thesis the author could not find publications related to information security education and awareness in developing countries except own publications.

d) *Security awareness strategy* – It was assumed that implementing security awareness program along with ICT deployment in organisations was the most effective way to ensure that societies in developing countries are well equipped with the basics of security.

e) *Author’s biasness* – Having worked in the ICT industry in Tanzania and neighbouring countries for at least 5-years prior to taking on this research, the author might have been influenced to some extent.
f) *Area of applicability* – The proposed DAISA approach is meant for organisations that have staffs and management hierarchies. It is not applicable to home users of IT systems or companies with two or less staff only.

These assumptions may be taken as limitations of this work. In this case we encourage other researchers to carry out similar researches elsewhere in developing countries in order to validate these assumptions. This has been left as part of future research.

**1.9 Contributions**

In broad terms, the main contribution of this thesis is the DAISA approach itself in the developing countries’ environment. This is because the approach has considered the current conditions and constraints in developing countries. The DAISA was systematically developed using a scientifically grounded methodology, action research McCutcheon and Jung (1990). The methodology is firmly founded on the General System Theory Bertalanffy (1968); Ackoff (1971) and Cybernetics Wiener (1948). It will serve as a guide to security awareness initiatives in those countries. This will eventually contribute to the overall mission of addressing information security awareness issues in developing countries, and perhaps elsewhere. Even though our case study was conducted in a developing country, we strongly believe that the proposed approach can be adopted and implemented in any other country. This is because the approach is dynamic and adaptive in its nature. Derived from the
main contribution, there are other associated contributions that are targeting specific groups as follows:

**To Business Organisations**
Business organisations that have been long awaiting a professional guide on the planning and implementation of security awareness programs at workplaces, here is the guide. Although it is apparently targeting organisations in developing countries, the approach can equally be adopted in any organisation elsewhere. This guideline is offered free of charge. It is a self-teach guideline to any interested entity. The thesis will be uploaded on the net for online access from anywhere around the globe. Also, the guide will serve as a basis not only for decision making but also for accounting on expenditures on security.

**To Governments**
Governments in developing countries like other organisations shall be able to adopt the approach to raise the security awareness of their employees in efforts to protect their information assets and critical infrastructures supporting it. This will not only protect governments’ information assets but also build trust and confidence of citizens when accessing government information online such as E-Government Services. Also, since most governments are relatively slower to adopt new changes through their bureaucratic procedures as compared to private business organisations, they should be able to learn from early adopters of the approach.
To IT Managers and Systems Administrators
For systems administrators and IT managers who were facing difficulties in persuading their managements to support security initiatives, the DAISA approach is a handy tool for the task. Using the DAISA approach as a guide they will be in a position to build business cases around security awareness and confidently present them to managements for scrutiny and endorsement.

To the Research Community
As stated earlier in this thesis there were scarcity of publications with respect to information security awareness (and security at large) in developing countries. We, therefore, believe that this research will trigger or prompt for many more related research activities elsewhere in developing countries. This work also, shall provide other potential researchers in the area with a comparative base of their findings.

To Individuals
Individuals who happened to attend one or more of our courses or seminars have benefited. This is another contribution of this research. In addition, all presentation slides; course materials; newsletter articles; and the Licentiate thesis are available online for everyone’s access. Moreover, this thesis shall be uploaded to the University of Dar es Salaam web site for public access. This way many other individuals will benefit from this research, hence wider outreach, which is one of the objectives of this research.
To the General Public

Many people in developing countries and elsewhere will have free online access to this thesis. This means that its outreach shall be as wide as possible. Thus, many people will benefit from the findings and subsequent implications of this thesis, hence raise their security awareness.

1.10 Thesis Layout

Chapter 1 is meant to set the scene or picture of the research. It gives an overview of and background to the research. Furthermore, it states the research problem and purpose, discusses research methodology and theoretical foundation of the research. The chapter finally summarises the contributions of the research and limitations of the work.

Chapter 2 is about information security in a bigger picture; from the definition to the value and importance of information security. It also discusses risks, threats and vulnerabilities in the context of information security. It is intended to give the reader a deeper and broader understanding of information security.

Chapter 3 discusses in details the entire research process. Specifically, the chapter describes in details the two phases the research has undergone including evaluations or validation of the first phase. It then outlines the key findings from the research that lead us to the proposed DAISA approach. Generally Chapter 3 outlines the basis and criteria for the DAISA approach.
Chapter 4 describes the empirical security survey. The chapter discusses the design, distribution, management and analysis of the questionnaires. Results from the questionnaires are also presented, discussed and interpreted in this chapter. Reflections from Chapter 4 contribute criteria for the DAISA approach.

Chapter 5 gives a summary of related publications (refereed papers) and other articles written by the author as part of this research. Comments gathered from conferences when presenting the papers coupled with suggestions and comments from the audiences that read the Newsletter articles form part of the content for the DAISA approach.

Chapter 6 presents and describes the design, content, and structure of the Dynamic and Adaptive Information Security Awareness (DAISA) approach. It also discusses the strategies for implementing the DAISA approach. Finally, the chapter discusses the validations of the DAISA approach using the action research methodology.

Chapter 7 summarises the thesis by reiterating the contributions made by this research and the concluding remarks. The chapter finally gives suggestions for future research in relation to this work.
Chapter 2

INFORMATION SECURITY IN A BIGGER PICTURE

Information security is a broad area that encompasses many interrelated sub systems from hardware to software, to data and information, to processes, to people. This chapter attempts to outline the broad spectrum of the subject starting by describing a conceptual IT system and defining information security in its broader sense. It further discusses risks, threats and vulnerabilities to information assets and their possible sources. The chapter also presents and describes security perspectives and security countermeasures. It also highlights some security evaluation criteria and security metrics standards in a nutshell, and finally it concisely describes a security learning continuum.

2.1 A Conceptual IT System

Prior to defining what information security is all about, we first describe a conceptual Information Technology (IT) system and its components. A conceptual IT system, as applied in this thesis, is a term that refers to a complex super system of passive and active sub systems. At a macro level a conceptual IT system comprises of three major components namely technology, people and processes. Figure 2.1 depicts a macro view of a conceptual IT System. Applying the concepts of the systems theory
Bertalanffy (1968); Schoderbek et al (1990); Ackoff (1971), we are referring to the higher level or rather a more abstract view of the IT system. At this level we are talking of the wholes without considering details of the parts neither environment.

![Figure 2.1 Macro View of a Conceptual IT System](image)

At a micro level we can see ‘Technology’ and ‘People’. The former includes hardware and software. The people category includes staff, customers, partners, ex-staff, temporary staff, competitors, suppliers, consultants, industrial espionage, hackers, and others. We, therefore, refer to these sub systems as components of an IT system. They all act on data or information assets stored in, processed or transmitted between computer systems. The interactions between people and technology when acting on or manipulating data or information are what we herein refer to as processes. Processes are sometimes referred to as throughput of the system. Figure 2.2 illustrates a generalised model of an IT system with data or information, people and technology as input components interacting in some ways to give output.
Figure 2.2 Generalised Model of an IT System

Let us briefly examine the three input components of the generalised model of an IT system.

**Technology** – Technology includes hardware components and software. Hardware consists of active devices, Perlman (2001), (i.e. devices that are configurable such as switches, servers, etc.); and passive devices (i.e. devices that are not configurable such as passive hub, etc.). Software includes Operating Systems (OS), Applications Software, and Firmware. Figure 2.3 depicts the constituents of the Technology component.
**Data and Information** – Data and information are two distinct entities. It is not uncommon that many people tend to apply the two synonymously. We define data as a conceptual representation of known facts with implicit meaning. This means that when we assign meaning to data it becomes information. Information is, therefore, the subjective interpretation of data. According to Gollmann (1999) data represents information. Gollmann (1999, pp. 11) defines data as

> “a physical phenomena chosen by convention to represent certain aspects of our conceptual and real world. The meanings we assign to data are called information. Data is used to transmit and store information and to derive new information by manipulating the data according to formal rules”.

Thus, collectively data and information include customer records, staff records, medical records, management information, business plans, budgets, intelligence information, payroll records, and the like. All user data falls into this category. Figure 2.4 illustrates a non-exhaustive list of data and information.
People – People are the most active, complex and dynamic component of an IT system. People in this context include staff, customers, ex-staff, suppliers, temporary staff, partners, consultants, industrial espionages, hackers, competitors, and other motivated attackers. If you look at the cross-sectional profile of people it includes insiders as well as outsiders. This leads to the conclusion that attacks to information assets might equally come from both within and outside the organisation. Figure 2.5 depicts people as one of the key components of an IT system.
Using Figure 2.3, Figure 2.4, and Figure 2.5 as basis one can easily see how complex an IT system is. It is this complexity that makes it difficult to clearly demarcate the boundary of an organisation’s IT system. The difficulty is mainly due to the fact that there are, essentially, at least four categories of people or entities that can have access to the organisation’s IT assets. These include:

1. Insiders (i.e. staff, temporally staff, consultants)
2. Outsiders with access to the inside (partners, suppliers, customers)
3. Outsiders with some knowledge about the inside (ex-staff, ex-consultants)
4. Outsiders with certain motivation to launch attacks against your organisation (competitors, hackers, industrial espionages, other attackers)
All these are potential attackers to the organisation’s information assets and resources. In this case, setting the boundary of your IT system is a critical step when attempting to protect it. It is not that easy though that is why an American ecologist of the 19th century John Muir once said that:

“When we try to pick up anything by itself we find it attached to everything in the universe”

–John Muir

We expand on this assertion by Muir to say that those entrusted to manage corporate IT systems should precisely define boundaries of their systems in order have a better control of the input.

Besides the long and extended definition of an IT system we have attempted to put up, many other authors in this area have attempted to define an IT system in many different ways. This is due to the fact that there is no standard definition of an IT system Gollmann (1999); Yngström (1996); Brenton (1999). The US national colloquium defines a computer system as an entire infrastructure, organisation, personnel, and components for the collections, processing, storage, transmission, display, dissemination, and disposition of information Reynolds (1998). In another closely related definition Anderson (2001) defines an IT system as also including staff, internal users and management, customers and other external users, policies and procedures, surrounding environment including the media, competitors, regulators, and politicians. Bruce Schneier in his book titled ‘Secrets and Lies’ Schneier
INFORMATION SECURITY IN A BIGGER PICTURE

(2000) had put it that security involves people, things people know, relationships between people, people and how they relate to machines; adding that security involves computers, that are complex, unstable, and sometimes buggy.

This broad definition of IT system is like this probably because the definers use or think about the system in a problem-oriented (i.e. security problems) way. In this thesis we shall, therefore, use the term IT system in its broadest sense.

Having looked at the definition of an IT system, its components, and possible sources of attacks, let us now see what information assets consists of.

2.2 Information Assets

Information assets sometimes referred to as information resources include hardware, software, and people that an organisation uses to perform computing tasks Pfleeger (1997). According to Chris Brenton even the time dedicated for the organisation’s business is counted as part of information assets Brenton (1999). An Information Security Guideline for NSW Government – Part 1 Information Security Risk Management, Issue No: 3.2 gives a much broader definition of information assets AusGuideline (2003, pp 14). The guideline defines an information asset as follows:
“An asset is something that the agency values and therefore has to protect. Assets include all the information and supporting items that an agency requires to conduct its business. Examples of these assets include:

1. Information/data (e.g. files containing payment details, voice records, image files, product information, manuals, and continuity plans);
2. Paper documents (e.g. contracts, completed forms);
3. Software (e.g. system software, application software, development tools and utilities);
4. Physical equipment (e.g. computer and communications equipment, magnetic media, other technical equipment such as medical equipment and environmental equipment, furniture, accommodation);
5. Services (e.g. computing and communications services, service providers, and utilities);
6. People and their knowledge (e.g. technical, operational, marketing, legal, financial, contractors and consultants, outsourced providers);
7. Image and reputation of the agency.”

Regardless of the wording used to describe information assets it can be noted that, in essence, it is a broad and somewhat complex term.

**2.3 Defining Information Security**

By definition information security is all about controlling access to information assets and resources and ensuring availability of these assets to legitimates users at all times. This is, however, a simplified definition of
information security. In more concrete terms information security involves controlling access to information assets to ensure confidentiality, integrity and availability (CIA) of the assets to legitimated users at all times Pfleeger (1997); Stallings (2000); Gollmann (1999). Figure 2.6 illustrates the three traditional facets of information security commonly referred to as security services.

From IBM Dictionary of Computing, Information Security is defined as the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use McDaniel (1994). A closer examination of the definitions for information security reveals that it all boils down to access control to information assets. It is all about protection of information assets against unauthorized disclosure, deletion, modification or alteration, fabrication, interruption or destruction, whether accidental, intentional or out of mere ignorance. Information security
also deals with issues of trust of entities with respect to access to information. The term also includes privacy of information.

Information Security is also defined by the International Standards Organization ISO-17799, in which is characterised as the preservation of:

- **Confidentiality** – ensuring that information is accessible only to those authorized to have access.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – ensuring that authorized users have access to information and associated assets when required.

In either case, outcomes of the security breach may include one or more of the following interruption, interception, modification or fabrication of data or information Pfleeger (1997), Stallings (2000, pp.6-9). These outcomes are illustrated in Figure 2.7.

- **Interruption**: – refers to a scenario in which an information asset is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting or somehow blocking of communication lines, or the disabling of the file management system.

- **Interception**: – refers to a scenario whereby an unauthorised entity gains access to an information asset. Interruption outcome is basically an attack on confidentiality. The unauthorised entity could be a person, a program, or
a computer. Examples include wiretapping to capture data in a network, and eavesdropping.

![Figure 2.7 Outcomes of Security Breach](Source: Stallings (2000, pp. 7)].

- **Modification**: refers to a scenario in which an unauthorised entity not only gains access but also tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.

- **Fabrication**: refers to a scenario whereby an unauthorised entity inserts counterfeit objects into the system. This is an attack on authenticity. Examples include the insertion of spurious messages in a network, hijacking a communication session or addition of records to a file. Man-in-the-middle attack is a typical example of fabrication.
2.4 Security Risks, Threats and Vulnerabilities

Security risks, threats and vulnerabilities are terminologies commonly used in the area of information security. In this section we shall attempt to describe them and their relationships in the context of information security.

Security Risk – refers to relative exposure of an information asset and the probability or likelihood that the asset can be compromised plus the possible loss Pfleeger (1997). The US national webcast initiative in its glossary of terms Webcast (2004, pp. 3) defines security risk as:

“Impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur”.

Threat – refers to circumstance that has the potential to cause loss or harm to an information asset Pfleeger (1997). A threat may be passive or active. Passive threats include release of message contents and traffic analysis. This includes eavesdropping on, or monitoring of transmissions of data through the network Stallings (2003, pp. 11). Passive threats usually have effects on confidentiality of information. Active threats as the name suggests involve actual contact with data or information and this might result in compromise of data integrity. Active threats include masquerade, replay, modification of message contents, and denial of service (DoS) Stallings (2003, pp. 12).
**Vulnerability** – refers to a weakness in an IT system which might be exploited to cause loss or harm to information assets Pfleeger (1997). The US national webcast initiative Webcast (2004, pp. 4) defines vulnerability as:

“A flaw or weakness in system security procedures, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in a harm to an IT system or activity”.

In security context, typical examples of vulnerabilities include software bug, hardware flaw, and of course security unawareness.

All these (i.e. risks, threats, and vulnerabilities) are closely related, and they usually coexist. Figure 2.8 illustrates their relationships.

![Figure 2.8 Relationships between Risks, Threats and Vulnerabilities.](Source: Australian Standard Handbook of Information Security Risk Management – HB231:2000]
Additionally, the DAISA approach proposed in Chapter 6 goes beyond teaching people to understand the risk concepts and their relationships. The approach requires the implementer, also, to educate the addressees on what to do in the event that a particular situation has occurred. For example, the awareness program in charge needs to tell the participants look, there is a virus threat out there and it does serious destructions to your data in a computer. Adding that, we need to get rid of this threat as much as we can. Here is antivirus software that has to be installed in every computer. The antivirus must be updated quite regularly, and preferably every one should configure it to automatic update. In case your computer has been infected by the virus, use the particular contacts to report the incident for immediate help. For all known threats it should be done in the same fashion. This way, users will gradually gain confidence and eventually their security awareness will increase with time.

Similarly, the Common Criteria for IT security evaluation discussed later in this chapter gives a more detailed map of the security contexts, risk concepts and their relationships as depicted in Figure 2.9.
What makes security a big challenge among professionals and experts in this area is its complexity. A potential attacker can be expected from any corner at any time to any IT system with any tools. Nonetheless any weak or simply most vulnerable parts of the system are the most frequent targets to attackers leading to what Charles Pfleeger refers to as the principle of easiest penetration. The principle states that Pfleeger (1997, pp.3):

“An intruder must be expected to use any available means of penetration. This is not necessarily the most obvious means, nor is it necessarily the one against which the most solid defense has been installed”.

Adding that,
“.... computer security specialists must consider all possible means of penetration, because strengthening one may just make another means more appealing to intruders” Pfleeger (1997, pp. 3).

Moreover, Donn Parker (2002) echoes this principle by saying that:

“The deadly serious game we play in information security is unfair. Attackers have a great advantage over the defenders. An attacker is intensively motivated to succeed in his one, selected, limited, and focused nefarious effort at a specific time and target and with no concern for collateral damage. The victim organisation must require all of their workers, contractors, partners, customers, and suppliers while they are trying to do their many assigned tasks to be alert and defend all vulnerabilities, all assets, at all times, and in all the varied work places from unknown attackers” Parker (2002, pp.1).

Charles Pfleeger complements to his principle of easiest penetration by offering another principle which he named the principle of adequate protection, stating that:

“Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value” Pfleeger (1997, pp. 9).

This principle requires that one should perform a risk assessment before implementing a particular security solution.
2.4.1 Security Attacks, Services and mechanism

Some of the key terminologies one may encounter in security literatures include security attacks, security services and security mechanisms. While literary might be meaning the same things, various literatures define them somewhat differently. For example, Stallings (2000, pp. 6-9) defines security attack as “*Any action that compromises the security of information*”. Adding that security attacks might be passive or active in nature. Also, Stallings (2000, pp. 4-5) defines security mechanisms as “*A mechanism that is designed to detect, prevent, or recover from a security attack*”. Similarly, Stallings (2000, pp. 9-11) defines security service as “*A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms*”. According to Stallings (2000, pp. 9-11) there are five security services namely:

- *Confidentiality* (informational privacy)
- *Authentication* (who created or sent the data)
- *Integrity* (has not been altered)
- *Non-repudiation* (the order is final, entity’s non-denial of participating into certain transactions or communications)
- *Access control* (prevent misuse of resources, allow legitimate use of resources)
- *Availability* (permanence at all times, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files
Note that: Texts in brackets are author’s interpretations of the meanings of the security services. Items in *italics* are the actual security services according to Stallings (2000).

In addition to the five traditional security services, some contemporary researches suggest *Accountability* as the sixth security service. Accountability in this context means ensuring that an action can be uniquely traced to the doer or the actor. Other literatures treat accountability as part of non-repudiation security service. As discussed earlier in this chapter, this is a real problem with most of terminologies used in the area of information security. Definers tend to describe terms in a problem-oriented way Yngström (1996); Gollmann (1999).

### 2.5 Security Perspectives

Various researchers have investigated information security in its entirety and came up with different views or perspectives. For example, Teemupekka Virtanen has observed security as existing in four views namely user’s view; developer’s view; organisation’s view; and scientist’s view Virtanen (2002, pp. 7-31). On the user’s view, Virtanen argues that a user is not only one of the most vital elements of information systems but also that a user is a customer who can make a choice on the type of services to buy. Under user’s view he considers social behaviour, issues of trust, privacy issues, and issues pertaining to educating users on how to use the IT systems properly and in a secure manner. He also argues that a user needs an ambassador in the cyber world because a user cannot act in that world; adding that trusted electronic
devices must translate electronic world to a user and perform functions a user wants to perform, like what an ambassador does in a physical world.

On developer’s view he looks at it from two different angles. One is the product that is being developed and the other is the development process. He argues that both the product itself and the development process have to consider security aspects right from the beginning. Under this view three aspects have been addressed including security as a requirement, security in the development cycle and secure development process. Figure 2.10 illustrates the four security views according to Virtanen (2002).

![Figure 2.10 The Four Security Views According to Virtanen (2002)](image)

Regarding the organisation’s view, Virtanen says security is a very important function at all hierarchies from an individual to organisation, to government, and to the world. Adding that at the organisation level is mostly the focal point in that most of security functions are done there. Furthermore, issues pertaining to organising security, organisational security, conflicts between security needs, and security cultures and evolution have also been addressed.
On scientist’s view, he looks at various research activities performed by researchers, academician, practitioners in the area, and other scientists, particularly, in conferences that are organised by the International Federation of Information Processing (IFIP) since its inception in 1960. He further, makes tracks comparisons, discusses contents of the conferences, and comments about scientific areas that have been presented and discussed at the conferences. He concludes that, in essence, security manifests itself in those four views and that it should be dealt with in those perspectives.

Moreover, Louise Yngström in a Systemic-Holistic Model views information security in a three dimensional perspective or framework Yngström (1996). Yngström argues that we need to view security related problems from:

1) Levels of abstraction;
2) Content/subject areas, and from
3) Context orientation.

On levels of abstraction, issues pertaining to physical constructions, theories & models, and design & architecture need to be looked at. Figure 2.11 depicts an overview of the Systemic-Holistic Model Yngström (1996, pp. 19).
Regarding content/subject areas there are technical aspects and non-technical aspects of security to be considered altogether. On context orientation issues such as specific context of implementation, geographical or space and time bound ‘system point’ have to be taken into account. In addition, Yngström introduces an epistemology element in the framework that she calls ‘the systemic module’. The framework taken together with the epistemology element or systemic module is what makes up a Systemic-Holistic Model.

2.6 Security Countermeasures

Besides the fact that you cannot make your system perfectly immune from attacks, there are always ways for improving the overall security of your IT systems or simply to make them less vulnerable. We need to work towards keeping our IT systems within acceptable limits of risks. Figure 2.12 illustrates risks vis-à-vis costs.
Effective security strategy must include both technical solutions and non-technical security measures Yngström (1996). Nonetheless, care must be taken before purchasing technical security mechanisms. Today there are numerous security technical mechanisms of which some are feasible but others are questionable. An organisation is advised to get a professional advice from a qualified and competent security practitioner beforehand. Technical solutions need to match the value of the asset it is intended to protect based on a comprehensive security risk assessment results. In addition, some technical solutions are not that reliable, and may cause even more risks to your systems.

Organisations have to implement a sort of a multilayered security approach Pfleeger (1997); Viega and McGraw (2002); Gollmann (1999), meaning that there should be proactive, detective, reactive and recovery security measures in place at all times. In any case, we argue that security awareness is
fundamental to all activities pertaining to protection of IT assets no matter how strong technical solutions may be.

2.7 Security Evaluation Criteria and Security Metrics

Business organisations dependent on IT systems requires some sort of assurance, be it from the product manufacturer or an independent trusted third party, that a product or system they are to purchase provides adequate security worthy their business values. In view of this, there have been various efforts to develop internationally acceptable security evaluation standards for different IT products and systems. A product or system being evaluated is referred to as a Target of Evaluation (ToE). Some of the most commonly known evaluation standards include the Common Criteria (CC), ISO/IEC 17799, and BS7799-2:2002.

The Common Criteria (CC)

Commencing in 1993, the Common Criteria project for information Technology Security Evaluation (CC) defines general concepts and principles of IT security evaluation and presents a general model of evaluation CCSE (2002). It, also, presents the constructs for expressing IT security objectives; for selecting and defining IT security requirements; and for writing high-level specifications for products and systems. The CC represents the outcomes of a series of efforts to develop criteria for evaluation of IT security that were broadly useful within the international community. Prior to the CC standard, the Trusted Computer System Evaluation Criteria (TCSEC), TCSEC (1983; 1985), was developed in the United States. It was commonly referred to as
‘The Orange Book’. In the succeeding decade, different countries began initiatives to develop evaluation criteria that built upon the concepts of the TCSEC but were, also, more flexible and adaptive to the evolving nature and trend of the IT field.

In Europe, the European Commission published the Information Technology Security Evaluation Criteria (ITSEC) version 1.2 in 1991 after being jointly developed by a consortium of France, Germany, the Netherlands, and the United Kingdom. In Canada likewise, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) version 3.0 was published in early 1993 as a combination of the ITSEC and TCSEC approaches CCSE (2002). Moreover, in the United States the draft Federal Criteria for Information Technology Security (FC) version 1.0 was also published early in 1993, as a second approach to combining North American and European concepts for the security evaluation criteria. Figure 2.13 shows the different evaluation criteria that merged to form the Common Criteria (CC).

Work had begun in 1990 in the International Organisation for Standardisation (ISO) to develop a set of international standard evaluation criteria for general use. The new criteria were meant to be responsive to the needs of mutual recognition of standardised security evaluation results in a global IT industry.
ISO/IEC 17799 and BS7799-2:2002

Published by the British Standards Institution for the UK (BSI), the BS7799 standard effectively came in two parts. The BSI first published a Code of Practice for Information Security in 1993 as PD0003. This was republished in 1995 as BS 7799. Subsequent discussions led to the publication of a standard for specification of requirements for an information security management system, as BS 7799 Part 2:1998. At that time the Code was renamed Part 1. Extensive discussions with industry, both in UK and abroad led to the first revision of the Code, published as Part 1:1999, accompanied by a consistent Part 2:1999.

BS 7799-Part1 was submitted to ISO as ISO/IEC DIS 17799-1, for fast-track approval to become an International Standard. In October 2000, it was approved and published by ISO as ISO/IEC 17799-1.

ISO/IEC 17799:2000 (Part 1) is the standard code of practice and can be regarded as a comprehensive catalogue of good security things to do. BS7799-2 is a standard specification for an Information Security Management Systems
(ISMS). The ISMS is the means by which Senior Management monitor and control their security, minimising the residual business risk and ensuring that security continues to fulfil corporate, customer and legal requirements. BS7799-2:2002 was published in September 2002 to replace BS7799-2:1999. Essentially, BS7799-2:1999 instructs on how to apply ISO/IEC 17799 and how to build, operate, maintain and improve ISMS. It also defines a six-step process in evaluating a ToE.

To cope with changing security needs for businesses and industry, the International Organisation for Standardisation (ISO) published a standard ISO/IEC 17799:2005: Information technology – Security techniques – Code of practice for information security management in June 2005 ISO/IEC 17799:2005 (2005). The standard was in response to the increased global business interconnectivity resulting into exposure of business information to a growing number and wider variety of threats and vulnerabilities. In particular, ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It, specifically, addresses best practices of control objectives and controls within the framework of information security management, including:

- Security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management
- compliance


Security Metrics

Published on April 1, 1999 Version 2.0 of the Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization’s security engineering process that must exist to ensure good security engineering Hefner (1999). In March 2002, Version II of the SSE-CMM was published by the International Standard for Organization (ISO) as Document ISO/IEC 21827 under the title: Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM) Lindquist (2002). It describes the characteristics essential to the success of an organization’s security engineering process and is applicable to all security engineering organizations including government, commercial, and academic. ISO/IEC 21827 covers the following aspects Hefner (1999); Lindquist (2002):

- Project lifecycles, including development, operation, maintenance, and decommissioning activities.
• Entire organizations, including management, organizational, and engineering activities.
• Concurrent interactions with other disciplines, such as system, software, hardware, human factors, test engineering; system management, operation, and maintenance.
• Interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation.

In June 2003 Version 3.0 of the SSE-CMM model was published McCulloch (2003). The primary objective of the SSE-CMM project was to advance security engineering as a defined, mature, and measurable discipline using standard security metrics. According to McCulloch (2003) security metrics are sort of quantifiable measurements of some aspect of a system or enterprise. In information security context metrics refers to any ‘identifiable attributes’ that collectively characterize the security of that entity. It is against such metrics that a particular security product, system or process is assessed.

Specifically, SSE-CMM outlines two types of metrics namely process metrics and security metrics. McCulloch (2003) defines process metrics as “Specific metrics that could serve as quantitative or qualitative evidence of the level of maturity for a particular SSE-CMM process area or could serve as a binary indication of the presence or absence of a mature process”. Whereas security metrics is defined as “A measurable attribute of the result of an SSE-CMM security engineering process, that could serve as evidence of its effectiveness.
A security metric may be objective or subjective, and quantitative or qualitative” McCulloch (2003).


2.8 Information Security Learning Continuum

Fundamentally, the information security learning continuum manifests itself into three major segments namely awareness, training and education Wilson (1998; 2003). Security awareness programs are meant to enable users to pay attention on security related issues such as risks, threats and vulnerabilities. Also, awareness programs are meant to enable ordinary end users to appropriately handle all security issues that do not require specialised technical knowledge. Learners in security awareness programs are somewhat passive in that they depend more on the trainers to get information.

Training is a more focused sort of programs that requires comparatively slightly advanced knowledge than awareness programs Yasinsac (2002). It is at training level where first level support technical staffs are prepared to handle some specialised technical assignments. Skills obtained at training level include installing, configuring, maintaining and troubleshooting various technical security mechanisms such as firewalls, intrusion detection systems, and the like. Usually, skills obtained through security training programs are
limited to a particular security product or system Yasinsac (2002); Wilson (1998; 2003). Learners in security training programs are relatively active compared to awareness. They are also expected to be more creative within their areas of competence. Various information security professional certifications fall under the training aspects of the security learning continuum.


2.8 Chapter Summary

This chapter has broadly highlighted information security in a bigger picture. Nevertheless, the area is too vast to be covered in a single thesis chapter. What has been covered so far is just the tip of the iceberg. To explore the entire area and acquire the necessary skills and better comprehension, references have been provided for your perusal. In general, the chapter has described an IT system, defined information security in its broadest sense; also it has presented various security perspectives, and highlighted security evaluation criteria and security metrics standards. In the end, the chapter has concisely described the information security learning continuum.
Chapter 3

DETAILED RESEARCH PROCESS

Based on our methodology and on the action-learning cycle in Chapter 1, this research has gone through two complete cycles or phases. This chapter describes the research process in details including activities done at each step of the two cycles. In addition, the chapter attempts to validate the work done in the phase 1 of the research. Finally, it outlines the impacts of security awareness seminars and short courses conducted during the research.

3.1 Phase One

Phase 1 of the research, also referred to as action-research cycle one, commenced by formulating the research question followed by deciding on the appropriate methodology to be applied. Given that we had no enough knowledge on the nature and magnitude of the problem we were attempting to investigate, we opted for an action research as discussed earlier in Chapter 1. Thereafter followed the actual execution of the research based on the chosen methodology. In the subsequent section we present and discuss the various research activities done in the course of this phase. We also, describe the evaluations of the first phase that gave a way to the second phase.
3.1.1 Activities in Phase One

Besides literature review and desk research, we conducted two information security awareness seminars. One seminar was specifically targeting IT practitioners from the industry while the other was special for academic and non-academic staff from the University of Dar es Salaam. In both events we dedicated an ample time for questions and answers (Q&A). It is through Q&A sessions that we collected useful feedback for our research. All sessions were interactive to allow for comments and suggestions from the participants. The IT practitioners’ seminar was attended by 65 participants; and 42 university staff attended the other seminar. From discussions and comments during the two seminars, and subsequent after-communications with the seminar participants several suggestions were made as follows below.

Summary of Seminar 1&2 Evaluations

In summary the following needs were recommended by the seminar participants, to:

- Conduct regular seminars of the kind in order to raise public awareness on IT security issues
- Introduce IT security to employees at their work places
- Integrate IT security into formal academic programs in the country
- Educate top managements on the importance of IT security to their organizations
- Incorporate IT security policy into corporate policies
- To develop independent IT security policies for their organizations
A detailed evaluation can be obtained in Casmir and Yngström (2003a) and Casmir (2003).

In addition to above mentioned seminars, we conducted a 2-day voluntary short course on IT security at the University of Dar es Salaam. The course attracted more than 200 students and tens of faculty members. The audience in the course was composed of students mainly from computer science, electronics and engineering disciplines. Also, a significant number of the students from other academic disciplines such as commerce and management, mathematics, education and a few from the faculty of law attended the course. During the course, we distributed and collected questionnaires for evaluation of the course. A sample questionnaire is attached as appendix A. At least 200 students responded to the questionnaires. Detailed analysis of these questionnaires is available in Casmir and Yngström (2003a) and Casmir (2003). However, some excerpt from the analysis is presented below.

**Summary of Course1 Evaluations**

About 200 students attended the course. This was far beyond our expectations as the course was voluntary and coincided with the exams period at the University. The course gave an overview of IT security including the security objectives. Security risks, threats and vulnerabilities were also discussed. On going through the questionnaires, the following were observed:
- Students were very much impressed by the course, and they indicated their appreciation of the material taught and the way it was presented to them.
- More than 78% had no idea about IT security concepts before.
- About 11% of students said they thought IT security was all about using strong passwords to prevent unauthorised access to data.
- More than 85% proposed IT security to be taught as part of their academic programmes.
- About 58% of the students wanted to know more about hacking techniques; some said they wanted to become ‘white hat hackers’ in future.
- Some students wanted to have hands-on training in the implementation of different security mechanisms, especially firewall implementations.
- Some wanted to learn more on cryptology in relation to IT security.
- Almost all students requested the course material to be made available, and if possible in electronic form. Almost all students who participated to the course expressed their interests and enthusiasm in learning more on IT security.

**Comments and suggestions from face-to-face interviews**

In addition, we conducted a number of face-to-face interview sessions with various stakeholders including IT managers and systems administrators from

---

1 In response to this, we uploaded both the course material and seminar material into a web server on the net (www.teil.udsm.ac.tz) for them to access. We granted them access to the material through Blackboard application software, an online software for e-learning.
different organizations; academic staff and students. The key findings out of these interviews include the need for:

- introducing IT security education at universities and other higher learning institutions in Tanzania
- promoting IT security awareness to reach as many computer users as possible in the country
- introducing IT security training and awareness at workplaces to minimise IT security risks in organisations
- devising ways for sensitising senior management in organisations to let them understand the importance of IT security, and make it one of the priority areas to strengthen
- organising frequent IT security seminars in the country to let practitioners exchange ideas on how to safeguard IT resources and assets

Comments and suggestions from conference participants

In the course of the first phase, two refereed papers were published as part of this work Casmir and Yngström (2003a) and Casmir and Yngström (2003c). Moreover, on presenting the papers we received some feedback comments and suggestions from conference participants. Some of the comments and suggestions from conferences’ participants include:
- To develop information security courses that can be incorporated within the existing academic programs such as computer science and computer systems engineering
- To develop security course materials that can be interweaved into the existing courses as separate topics
- To think of ways in which course instructors may discuss various security aspects including computer ethics when teaching non-security courses
- To think of developing a graduate-level curricula specializing in information security
- To consider inviting to Tanzania other experienced security researchers and educators to give security lectures as guest lecturers

3.2 Key Findings in Phase One

On aggregate there were at least three key findings on this phase namely:

1. The need for establishing academic program(s) for information security in Tanzania
2. The need to promote further security awareness in the country
3. To work out an effective way for implementing security training and awareness at workplaces

We arrived at these findings after consolidating comments and suggestions collected at different stages and evaluations of the course and seminars.
3.3 Output of Phase One

Based on evaluations of the seminars and short courses; comments and suggestions from interviewees; conferences’ participants; literature review; and on our personal experience in the area we came out with the output of the first phase. The first phase output was in the form of undergraduate-level information security curricula. The curriculum was aimed at exposing students to the appropriate and state-of-the-art tools and techniques that deter, detect, protect and react to the risks, threats and vulnerabilities to information assets. In addition, the curriculum was emphasizing on equipping students with both firm theoretical foundation on security concepts and appropriate hands-on practices. The curricula had the following main objectives to:

a) introduce students to the information security concepts in a holistic perspective
b) give students opportunities to develop their professional approaches in the area of information security
c) provide students with a structured and conducive learning environment to enable them to develop their individual abilities to manage information security in organisations at all levels (i.e. operational, tactical and strategic levels)
d) enable students build-up skills necessary to conduct research and development projects that are relevant to protection of information assets within their environments
e) promote awareness of the nature, capability and limitations of various security tools and techniques in the protection of information assets against various threats and vulnerability
f) facilitate the exchange of information regarding cyber threats, technology, tools, and other relevant issues with other researchers elsewhere

It was expected that universities and other higher learning institutions would adopt and implement the curricula. In this case we submitted copies of the curricula to at least 2 potential higher learning institutions in Tanzania for their scrutiny and implementation. Further details about the curricula are available in Casmir (2003). Additionally, the curricula gave flexibility in the implementations. According to Vaughn (2000) three implementation alternatives were made available as follows:

i. Incorporating security topics within existing courses
ii. Integration of security courses into existing academic programs, or
iii. Adopting the curriculum in its status quo (i.e. a security-focused curriculum) or with some amendments as it may deem necessary

All the three options were left for the implementing institutions to choose from. Combining two or more of the three options was also a possibility. Table 3.1 gives a summary of the main activities in phase 1 including the main output.
Table 3.1: Summary of Research Activities in Phase 1

<table>
<thead>
<tr>
<th>S/N</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Seminar 1</td>
<td>IT Practitioners</td>
</tr>
<tr>
<td>2</td>
<td>Seminar 2</td>
<td>UDSM Staff</td>
</tr>
<tr>
<td>3</td>
<td>Short Course 1</td>
<td>UDSM Students</td>
</tr>
<tr>
<td>4</td>
<td>Interviews</td>
<td>Practitioners, faculty members &amp; students</td>
</tr>
<tr>
<td>5</td>
<td>Publications</td>
<td>2-Refereed Publications</td>
</tr>
<tr>
<td>6</td>
<td>Phase 1 Output</td>
<td>Undergraduate Information Security Curricula</td>
</tr>
</tbody>
</table>

Key: UDSM – University of Dar es Salaam.

Development of the curricula concluded the first cycle of our methodology, which in turn, initiated the second phase cycle as shown in Figure 3.1.

![Phase 1 Cycle Complete](image)

**Figure 3.1: Output of the Phase One**

Generally, in phase 1 we fully addressed key finding number 1 and partly key finding number 2 in section 3.2. There are many reasons for choosing to address key finding 1 first. However, the most obvious ones were that:

a) An academic degree program focusing on ‘Information Security’ had higher potential for aiding other segments of the security learning continuum such as training and awareness.
b) The expected exit competencies from the program would be sufficient enough to meet expectations of many employers.
c) Students following the program would have ample time to learn the theoretical concepts of security as well as hands-on practices.
d) Students would gain enough knowledge to enable them carry out research in security after graduating from this program.
e) The program would not interfere with existing, already full, curricula.
f) In the long run it could have higher multiplying effect and greater outreach due to the fact that graduates from this program were expected to retrain others at their respective workplace.

Completion of the first phase of the research automatically triggered the beginning of the second phase. The first step in the second phase commenced with assessment and evaluation of phase 1. It was necessary that we do one more round of the research in order to see whether we were on the right track towards fulfilling the purpose of the research.

3.4 Phase Two

Phase 2 of the research was aimed at addressing the key finding number 3 ‘Security awareness at workplace’ at the same time partly address key finding number 2 to further promote security awareness to the general public. However, there were two issues to look at first. One was that we wanted to assess the work done in phase 1; and secondly it was not clear how we could go about addressing the challenge of introducing security awareness at workplaces. We dealt with the former using a group of 40 IT practitioners
from different organizations that convened as a ‘focus group’. Regarding security awareness at workplaces we applied a combination of more than one means to arrive at the proposed approach; means applied include writing refereed publications and collecting comments from conferences’ participants; face-to-face interviews with various stakeholders; conducting many more security seminars; running more security short courses; and using questionnaires. The latter is discussed in Chapter 4 whereas the rest of the activities are discussed in the succeeding sections of this chapter.

3.5 Evaluation of Phase One

A security focus group of 40 participants was involved in the appraisal of the output of the first phase. The group that convened for 5-days had three main objectives to accomplish. The first objective was to learn more on information security issues and trends, and the second objective was to assess the viability and effectiveness of disseminating security knowledge through different methods or approaches. The third objective was, essentially, inherent in the second objective. This was to validate the work done in phase 1 of the research.

We supplied the participants with nearly the same questionnaire prior to commencement of the training program, and at the end of the program with differences in the first questions. In the pre-training questionnaire, the first question was aimed at capturing expectations of the participants out the training program they were about to start. In the post-training questionnaire, the first question was aimed at tracking whether the program met their
expectations satisfactorily. Samples of questionnaires are attached as Appendices B and C respectively. Table 3.2 shows the composition of participants in the focus group.

<table>
<thead>
<tr>
<th>Category</th>
<th>No. of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Institutions</td>
<td>9</td>
</tr>
<tr>
<td>Government Agencies</td>
<td>8</td>
</tr>
<tr>
<td>Academia</td>
<td>5</td>
</tr>
<tr>
<td>Private Org./NGOs</td>
<td>18</td>
</tr>
</tbody>
</table>

### 3.5.1 Pre-Training Evaluation

As it can be seen from the pre-training questionnaire in Appendix B, there were 4 questions. In question one we asked participants to jot down their expectations out of the 5-day security training program they were about to start. Responses to this question are presented in Table 3.3. There were nearly as many expectations as the number of participants.

<table>
<thead>
<tr>
<th>S/N</th>
<th>Expectation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>What is IT Security</td>
</tr>
<tr>
<td>2.</td>
<td>Standards available for IT Security</td>
</tr>
<tr>
<td>3.</td>
<td>Responsible for Security Standards/ Compliance</td>
</tr>
<tr>
<td>4.</td>
<td>How to apply IT Security</td>
</tr>
<tr>
<td>5.</td>
<td>Challenges of IT Security</td>
</tr>
<tr>
<td>6.</td>
<td>Opportunities of IT Security</td>
</tr>
<tr>
<td>7.</td>
<td>Privacy in relation to IT Security</td>
</tr>
<tr>
<td>8.</td>
<td>How to handle computer /Network attacks</td>
</tr>
<tr>
<td>9.</td>
<td>Freedom of expression vs IT Security</td>
</tr>
<tr>
<td>10.</td>
<td>IT Security vs traditional Security</td>
</tr>
<tr>
<td>11.</td>
<td>How reliable is IT Security</td>
</tr>
<tr>
<td>12.</td>
<td>Importance of IT Security</td>
</tr>
<tr>
<td>S/N</td>
<td>Expectation</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13.</td>
<td>Importance of IT Security prevention measures</td>
</tr>
<tr>
<td>14.</td>
<td>Risks associated with IS/IT system</td>
</tr>
<tr>
<td>15.</td>
<td>Why worry about IT Security</td>
</tr>
<tr>
<td>16.</td>
<td>Developing a corporate IT Security policy</td>
</tr>
<tr>
<td>17.</td>
<td>Cost of IT Security</td>
</tr>
<tr>
<td>18.</td>
<td>Laws governing IT Security in Tanzania and elsewhere</td>
</tr>
<tr>
<td>19.</td>
<td>Security incidents and case studies</td>
</tr>
<tr>
<td>20.</td>
<td>When, where and how to apply IT security</td>
</tr>
<tr>
<td>21.</td>
<td>How to start IT Security Consultancy business</td>
</tr>
<tr>
<td>22.</td>
<td>IT Security certification and how many are available in the word market</td>
</tr>
<tr>
<td>23.</td>
<td>IT Security Approval</td>
</tr>
<tr>
<td>24.</td>
<td>How big is Cyber threat/ risks Vs Y2K</td>
</tr>
<tr>
<td>25.</td>
<td>Who is responsible for IT Security in an Organization</td>
</tr>
<tr>
<td>26.</td>
<td>What are tools available to ensure in interoperability of various- IS/ IT</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td>27.</td>
<td>Success factors for Security</td>
</tr>
<tr>
<td>28.</td>
<td>Are there off-the-shelf packages for IT Security?</td>
</tr>
<tr>
<td>29.</td>
<td>Is IT Security a “Black box” or something else?</td>
</tr>
<tr>
<td>30.</td>
<td>Is it possible to have it for own use?</td>
</tr>
<tr>
<td>31.</td>
<td>Is IT Security an Open Source or ----</td>
</tr>
<tr>
<td>32.</td>
<td>How is IT Security affecting our daily lives?</td>
</tr>
<tr>
<td>33.</td>
<td>Future expectation of IT Security</td>
</tr>
<tr>
<td>34.</td>
<td>Which languages is IT Security available in</td>
</tr>
<tr>
<td>35.</td>
<td>Information classification in an organization</td>
</tr>
<tr>
<td>36.</td>
<td>Is IT Security sharable?</td>
</tr>
</tbody>
</table>

Question 2 was aimed at assessing the effectiveness of different methods or approaches in the dissemination of security knowledge in Tanzania. Essentially, with this question we wanted to assess our approach proposed in phase 1. However, this was not revealed to the respondents to avoid pre-empting their responses. Responses to question 2 are presented in Table 3.4. Participants were asked to rank the methods from 1 to 5. Meaning that a method or approach ranked 1 was the most effective and that ranked 5 was the least effective in that fashion.
Table 3.4: Rankings of the effectiveness of IT security Education/Training Methods

<table>
<thead>
<tr>
<th>Effectiveness Rankings</th>
<th>IT Security Education/Training Method:</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SM/WS</td>
<td>SACP</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
<td>0</td>
</tr>
</tbody>
</table>

**Key:**
- SM/WS – Seminars/Workshops
- SACP – Specialised IT Security Academic Program
- TWP – Security Training at Workplace

Participants were also asked to give reasons especially for their ‘best’ and ‘least’ choices respectively. The following below are the reasons given by respondents.

(i) **Reasons for the best choice**

➤ *In favour of TWP*

- Workplace security training is the best in my view since nearly all employees will get a chance hear to about security
- Even the management can see for themselves the importance of IT security and fund it
- Employees will understand better the security concepts if the training is directed to their day-to-day job functions
- It is cheaper to train people at their work places
- Employers do not easily let staff leave their work stations to the seminars for quite long so better if it is done at the respective workplaces
- I think at a workplace more people will participate in the security training programs
- Also, the members of the management can get trained if this is done at a workplace

**In favour of SACP**
- Specialised IT security degree program will attract more students especially at this time when IT security is still a hot cake in Tanzania
- Academic program in IT will help to produce our own local security experts
- I think we need university level education in IT security in order to keep pace with changing security threats in the world of ICT

**In favour of both TWP+SACP**
- It is better to combine both
- University security education is important so is security training at workplace, let us combine them

**(ii) Reasons for the least choice**
- Seminar gives only overview of security not details
- Seminars and workshops are usually for promotion of security not for training and education, at least to my understanding
- IT security seminars and workshops should continue but more specialised security training program should be developed
We cannot rely on seminars to disseminate IT security knowledge to the whole country, after all seminars are attended by just a few individuals, the majority at large remains unaware of security issues.

Question 3 required participants to rate the ‘necessity’ and ‘urgency’ of IT security education and training in Tanzania. Responses to this question are presented in Table 3.5.

Table 3.5: Responses on the Necessity and Urgency of IT security Education/Training in Tanzania

<table>
<thead>
<tr>
<th>Response</th>
<th>No. of Respondents</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Necessary but not urgent</td>
<td>14</td>
<td>35%</td>
</tr>
<tr>
<td>Urgently necessary</td>
<td>26</td>
<td>65%</td>
</tr>
<tr>
<td>Not necessary at the moment</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

Question 4 required participants to give any other comments or suggestions with respect to IT security education and training in Tanzania. However, we got no general comments from questionnaires. It seemed participants did not have much to comment on before the actual training starts. Also, many were eagerly waiting for presentations on security.

3.5.2 Post-Training Evaluation

As mentioned earlier the first question in the post-training questionnaire was meant to assess whether participants’ expectations had been met satisfactorily. Table 3.6 presents responses to this query.
Table 3.6: Level of Satisfaction from the Training Program

<table>
<thead>
<tr>
<th>Response</th>
<th>No. of Respondents</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, completely</td>
<td>38</td>
<td>95%</td>
</tr>
<tr>
<td>Yes, about 75%</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>Yes, about 50%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Not at all</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

A second question was essentially meant to assess this work, especially, the output of phase one. Responses to question 2 are presented in Table 3.7. Like in the previous case, participants were required to rank the effectiveness of the method or approach in dissemination of security knowledge in Tanzania. Rank 1 designated as the ‘most’ effective and 5 as the ‘least’ effective method.

Table 3.7: Rankings of the effectiveness of IT security Education/Training Method

<table>
<thead>
<tr>
<th>Effectiveness Rankings</th>
<th>IT Security Education/Training Method:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SM/WS</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>35</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
</tbody>
</table>

Key:  
SM/WS – Seminars/Workshops  
SACP – Specialised IT Security Academic Program  
TWP – Security Training at Workplace

Similarly, participants were requested to give reasons for their ‘best’ and ‘least’ choices. Following below are reasons given for these choices.
(i) Reasons for the best choice

⇒ In favour of TWP

- Training at workplace will provide opportunity for many people to learn
- Many people will be trained at workplaces
- It is better to learn security within your work environment
- Not many reaches university level, better at workplaces
- University education is more theoretical, learning at work will be more practical
- It will take long to wait until one finishes a university degree, let us start now at workplaces
- It is relatively cheaper to do it at workplaces
- Security training at workplaces will be more focused on our day-to-day work
- At the university only few will be trained/educated in Security, I think better at workplaces or both
- At the university only those doing IT security degree program will benefit, whereas at work every employee will benefit
- IT security need real-life experience on the job, university education especially in Tanzania is too theoretical and I do not see it changing soon
- Getting a new degree program in IT security implemented will take ages, the way I know our universities in Tanzania, let it be done at workplaces and may be later at the university
- As you said in one of your presentations, IT security is context-dependent so it will be more effective if it is implemented at a specific work area.
- It is easier to learn while working, most of university students do not know specifically which job they are going to do after graduation, I suggest that IT security training at workplaces is much better.
- Let us implement it at work it is easier and more practical than at the university where it will be mainly simulation of ideal situation.

➔ In favour of SACP
- It is much better to do IT security as a specialised academic program in order to get an in-depth understanding of the area.
- At the university level is where one gets the highest knowledge so if Tanzanians are to learn and understand IT security concepts it should be done as a specialised academic program.
- I think graduates from a specialised IT security academic program will influence and spearhead security in organisation, so university degree in security is my favourite choice.
- If IT security is done as a specialised academic program, it is easier to develop security research topics, also funding of research is much easier in academic environments than in business.
- Universities are incubators of all experts around the world therefore to get our own security experts in Tanzania it should be done at the university.
- We need many people with university degrees in IT security in Tanzania so that they can train others, we should not over-depend on external aids even on IT security. It is high time that universities should introduce IT security as one of their degree programs.

🎉 In favour of both TWP+SACP

- Combining university graduates in IT security with other IT security technicians or lower level security personnel is a better idea to me.
- Although I’m not an IT security expert, but I think from my little knowledge university graduates in IT security will have their role to play which is most probably different with that of lower security knowledge. I think we need to combine the two.
- University graduates from IT security degree programs will do research oriented security and new inventions in security solutions, and let businesses and other organisations use or implement their research results. In this case implementers of the research results may not necessarily be graduates in security but people with general knowledge of security.
- We need both university IT security education and business oriented/focussed security knowledge.
- Since it might take long to wait for the first output from our universities, then I think it is better to do both simultaneously a university degree program for security and ordinary security training at workplaces.
- The world of ICT advancement and IT security is not waiting for us (Tanzanians) so let us do both academic security programs and workplace training
- As we have learned about IT security in this program, I suggest that we apply both academic and at work security training
- I think IT security training at workplace and academic security education will yield better fruits than implementing one approach only

(ii) Reasons for the least choice
- Seminars and workshops are costly
- Organising seminars is time consuming
- Seminars attracts heterogeneous audiences so the security knowledge we get is too generic, we need focused IT security knowledge
- Seminars and workshops are both time consuming and cost intensive
- It is not easier to always be permitted by the employer to attend seminars, especially if it is lasting longer like this one
- In seminars and workshops we end up getting introductory parts of topics, we do not get the entire security knowledge. For example, this is my second time I am attending security seminars that are organised by the University of Dar es Salaam Computing Centre but my security knowledge is still not as much as I expect it to be
- Seminars take shorter time but security seems to be broader than the time allocated for seminars, that is why I suggest it to be done at work
- Only a few people can get information about a particular IT security seminar, and sometime the notice is too short for some people to attend therefore they tend to miss it.
- People from upcountry’s office normally do not get chances to attend security seminars since many are done in Dar es Salaam only, better to do the training at workplaces as I suggested earlier.
- Seminars do help to raise security awareness but not as effective as when this could have been done at workplace.
- IT security seminars are mainly attended by IT staffs, but as you mentioned in your presentation every employee in the organisation need to have some IT security knowledge though at varying degrees of depth.
- Seminars are useful in promoting security but not for actual knowledge gaining, therefore it is the least effective way for IT security knowledge dissemination over other methods mentioned.

Likewise, in question 3 participants were requested to rate the ‘necessity’ and ‘urgency’ of information security education and training in Tanzania. Responses to this question are presented in Table 3.8.

**Table 3.8: Responses on the necessity and urgency of IT security Education/Training in Tanzania**

<table>
<thead>
<tr>
<th>Response</th>
<th>No. of Respondents</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Necessary but not urgent</td>
<td>1</td>
<td>2.5%</td>
</tr>
<tr>
<td>Urgently necessary</td>
<td>39</td>
<td>97.5%</td>
</tr>
<tr>
<td>Not necessary at the moment</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>
In question 4 participants were requested to give any other general comments with respect to information security education and training in Tanzania. Following below are the general comments given.

**Other general comments:**

- IT security is a very important issue especially now in Tanzania, as you see many computers are being imported some are not good but we cannot know which are good and which are not
- Teaching security at workplaces is an excellent idea, however, many people out there are adults and do not have computer background
- In the Internet there are many good things and bad ones so IT security education is urgently needed to enable Tanzanians to distinguish between good and bad Internet contents
- Every time computers are attacked by virus and a few people know how to get rid of the virus threats therefore I think IT security knowledge is required especially on the issue of viruses
- May be also the government of Tanzania should look at the issues of IT security as a national concern to give it more weight, I think
- Universities should play a key role to promote IT security and to produce security experts in the area
- I commend you Mr Respickius for your good and comprehensible presentations, and the University Computing Centre for introducing these sorts of seminars to open up our mind on IT security. I doubt if many people in Tanzania are aware of IT security issues and trends. It
seems to me many are just enjoying using the Internet without knowing its dangers

- I suggest that you should be organising these types of seminars to let more people understand or at least get overview of IT security concepts. I know it is expensive to organise them but please when you get funds just do it or perhaps a better way could be to ask participants to meet the seminars costs and you only offer them the security knowledge for free. I would be prepared to meet my own cost. Make it shorter, say 2 to 3 hours so that you do not incur costs for meals and drinks

- Try to liaise with potential organisations such as banks and government agencies to see if you can run security seminars for their staffs at their premises, I think this can be one of the cost effective way of disseminating security knowledge

3.5.3 Reflections on the Evaluations

Two rounds of evaluations were made for mainly two reasons. One was that in the pre-training evaluation we wanted to get the ‘actual’ feeling of the participants on information security before telling them anything about it. In addition, we did not want to pre-empt their responses on the questions in the questionnaires through our presentations on security. The second reason was that in the post-training evaluation we wanted to see whether security knowledge gained during the 5-day training had changed their thinking on security at all.
It was observed from Table 3.4 that 62.6% of the participants ranked security training at workplace as the most effective way to disseminate security knowledge in Tanzania. A combination of training at workplace and a specialised security academic was ranked second with 20% of respondents supporting it as the most effective approach. In this round specialised security academic program only was ranked third with 17.5% of respondents in its favour. None of the participants ranked security seminars and workshops as the first or second most effective method in the first round. Interestingly, all of the respondents ranked the use of security seminars and workshops as the least effective approach.

In the second round (i.e. post training evaluation) security training at workplace was even further supported by a larger margin of 77.5% of the respondents in Table 3.7. Like in the first case a combination of training at workplace and academic curricula emerged second while an academic curriculum alone was third. Likewise none of the respondents ranked security seminars and workshop as either first or second best method. Similarly, all ranked seminars and workshops as the least effective approach for dissemination of security knowledge in Tanzania. From these reflections it can be concluded that there was a need to work out an approach for establishing information security training at workplaces. Also, that it was important to have a combination of training at workplace coupled with academic specialised security program.

Regarding the necessity and urgency of security education and training in Tanzania, 65% of the respondents said it was urgently necessary in the pre-
training evaluation while 35% said it was necessary but not urgent. None of the respondents said it was not necessary at the moment. Interestingly, nearly all, 97.5%, of the respondents said it was urgently necessary in the post-training evaluation. Only 1 respondent said it was necessary but not urgent in this round, and none said it was not necessary at the moment. Other comments and suggestions from participants are self-explanatory.

3.6 Key Findings from Evaluation of Phase One

At least three key findings were noted from the evaluation of the first phase of the research.

1. The work done in the phase 1 was commendable but the timing was apparently not proper. More promotion of security awareness was required.

2. Information security training at workplaces was critically important. An appropriate approach for this was needed.

3. A combination of security training at workplace together with academic degree program focusing on information security was a more feasible approach to effectively disseminated security knowledge in Tanzania.

3.7 Other Research Activities in Phase Two

Besides the validation of phase 1, we continued with other related research activities in the second phase. Activities accomplished during phase 2 include more security seminars; more short courses; more related publications; further face-to-face interviews; and empirical survey using questionnaires. The latter
is presented and discussed at length in Chapter 4. Likewise summaries of related publications including refereed papers in international conferences and Journal are presented in Chapter 5. The rest of the activities are discussed in the succeeding sections of this chapter.

3.7.1 Seminars, Courses and Refereed Publications

In the course of the second phase of the research we conducted 3 more security short courses in addition to 1 course that was done in phase 1 of the research. We also conducted 8 more security seminars in addition to the 2 conducted in phase 1. One of the eight seminars in this phase was special for ‘senior executives (CEOs) and decision makers’ from different organisations in Tanzania. Moreover, we wrote 3 more publications (i.e. refereed papers): 2 in international conferences Casmir and Yngström (2004); Casmir and Yngström (2005); and one in the international Journal of Information Warfare Casmir and Yngström (2003c). Summaries of these papers are presented in Chapter 5.

3.7.2 Publications in Periodicals

As part of educating the society and creating more awareness, we published security articles on the University of Dar es Salaam Computing Centre’s Newsletters (ISSN 0856-9673). This is a quarterly periodical which is widely read within the country. After introducing security articles discussing various security topics, the Newsletter has attracted the vast majority of readers creating more demand on the copies produced. Originally, 1000 copies were
being produced per issue, but due to increase in demand due to security articles the production has been doubled to 2000 copies per issue. So far we have published 5 articles of which summaries are made in Chapter 5. This has extended the outreach in terms of fulfilling the integrated learning continuum which is the purpose of this research.

3.7.3 Interviews

We also, continued with face-to-face interviews with various stakeholders aimed at getting their insight about our approach to the research.

In an interview with one senior professor from the University of Dar es Salaam in Tanzania, he gave the following comments “Probably you made a miscalculation in developing [information] security curricula before the society [Tanzania’s society] was sensitised enough about security. You know having good curricula in place is one thing and getting it accepted and successfully implemented is quite another. You first need to have someone with a better understanding on security issues to push the idea forward. I doubt if many at this university and other institutions in Tanzania really understand what IT security is all about”. Making a reference to himself as a good example of many who do not understand IT security well. “Of course I know and have encountered [computer] virus several times, and I hear a lot about hackers, but I don’t think that’s all about [information] security. I think it is a lot more than that”. He further suggested what he called ‘aggressive sensitisation’ on IT security as the way forward to promoting security awareness in the country. Adding that, “I’m not saying having the IT security
curricula is bad, but all I’m saying is that it [the curricula] needs to be complemented with serious security awareness initiatives for better outcomes”. Earlier he was asked to comment on whether that was an appropriate time to introduce information security curricula at universities in Tanzania.

Apart from the comments and suggestions from that professor, we got many other constructive comments and suggestion from other people all of which have been incorporated into our proposed DAISA approach discussed in Chapter 6. One of the comments given by nearly all interviewees was that management in organisations were not adequately aware of IT security problems.

3.8 Key Findings in Phase Two

Key findings in phase 2 relatively do not differ much with those in phase 1. Findings in this phase include the following:

1. Security awareness was the most critical success factor and fundamental to security initiatives.
2. Security education and training was urgently necessary in Tanzania.
3. Academic program focusing on security was as equally important as security training at workplaces.
4. There was an urgent need to work out a method or an approach for introducing security awareness at workplaces.
5. Security awareness seminars were important in sensitising the society on security issues.
6. There was a need to create security awareness, specifically, to senior managements.

7. A combination of academic security program together with security at workplaces was considered the most effective approach to disseminating security knowledge in Tanzania.

3.9 Output of Phase Two

At the end of the second round cycle of the research we came out with ‘A Dynamic and Adaptive Information Security Awareness (DAISA) Approach. The approach is built on 6-pillars namely:

1) Management Support
2) Effective Communication
3) Security Motivation
4) Appropriate Planning
5) Relevant Training Material
6) Continuity and Consistency

These are considered as the critical success factors for introducing and maintaining security awareness at workplaces. Detailed discussions on the DAISA approach are presented in Chapter 6. Table 3.9 presents a summary of activities done in phase 2 of this work including the output. Figure 3.2 depicts the output of phase 2 of the research.
Table 3.9: Summary of Research Activities in Phase 2

<table>
<thead>
<tr>
<th>S/N</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Seminar 3</td>
<td>Senior Executives (CEOs)</td>
</tr>
<tr>
<td>2</td>
<td>Seminar 4</td>
<td>Staff and Students –UCLAS</td>
</tr>
<tr>
<td>3</td>
<td>Seminar 5</td>
<td>Staff and Students – SUZA</td>
</tr>
<tr>
<td>4</td>
<td>Seminar 6</td>
<td>Staff and Students – AIA</td>
</tr>
<tr>
<td>5</td>
<td>Seminar 7</td>
<td>Local + Internationals – DICC</td>
</tr>
<tr>
<td>6</td>
<td>Seminar 8</td>
<td>IT Practitioners – DICC</td>
</tr>
<tr>
<td>7</td>
<td>Seminar 9</td>
<td>Civil Servants – GDLC</td>
</tr>
<tr>
<td>8</td>
<td>Seminar 10</td>
<td>IT Practitioners – COSTECH</td>
</tr>
<tr>
<td>9</td>
<td>Short Course 2</td>
<td>Students – UDSM</td>
</tr>
<tr>
<td>10</td>
<td>Short Course 3</td>
<td>Students – UDSM</td>
</tr>
<tr>
<td>11</td>
<td>Short Course 4</td>
<td>Students - UCC Arusha</td>
</tr>
<tr>
<td>12</td>
<td>Interviews</td>
<td>Practitioners, faculty members &amp; students</td>
</tr>
<tr>
<td>13</td>
<td>Publications</td>
<td>3-Refereed Publications + Newsletter Articles</td>
</tr>
<tr>
<td>14</td>
<td>Security survey</td>
<td>Empirical results from security survey (Chapter 4)</td>
</tr>
<tr>
<td>15</td>
<td>Phase 2 Output</td>
<td>DAISA Approach</td>
</tr>
</tbody>
</table>

**Key:**
- GDLC – Global Development Learning Center – Tanzania
- COSTECH – Commission for Science and Technology – Tanzania
- DICC – Dar es Salaam International Conference Centre
- AIA – Arusha Institute of Accountancy
- UCLAS – University College of Lands and Architectural Studies
- UDSM – University of Dar es Salaam
- UCC – University Computing Centre
- SUZA – State University of Zanzibar

![DAISA Approach](image)

Figure 3.2: Output of Phase Two
3.10 Impact of the Research Activities

Security awareness seminars and short courses have had an enormous impact as far as security awareness is concerned in Tanzania. Effects of the security awareness seminars and short courses can best be viewed using Kowalski (1994) Socio-technical System model in Figure 3.3. Based on Kowalski’s socio-technical system model, we can see that introduction of security awareness seminars has positively impacted ICT culture. This in turn has affected the methods in which organisations handle their information assets. Today there are a number of job adverts for information security professionals in the local newspapers in Tanzania. This was not there before we started our security awareness seminars in year 2001. Therefore we count on it as partly influenced by the seminars. Introduction of the post of information security officer has, therefore, changed structures of organisations in question.

Also, tender adverts for security audit are being made in newspapers again this might have been influenced by our seminars to a larger extent. In at least three different instances, the author was invited to give specialised security awareness seminars in 3 distinct organisations in Tanzania. We tend to believe that was also an impact of our seminars and short courses. In every corporate ICT policy that is developed nowadays there is a section on information security. Likewise for those ICT policies that did not have such a section in first place, it is being added during policy review.
All these make us to conclude that they have been influenced by our seminars and short courses to a larger extent. The reason for drawing this conclusion was that in nearly all organisations where such changes happened, you find that there was one or more staff who had attended to one or more of our seminars. Kowalski (1994, pp.10) argue that any change in one of the 4 components of a socio-technical system disturbs the stability of the entire system. In this case, the system keeps on trying to maintain a certain degree of stability and control to regain its equilibrium state. Table 3.10 provides a summary of all security awareness seminars and short courses during the entire research including details of venue, duration, audience and number of participants. In each of these events we discussed various aspects of IT security. Topics were specific and were, actually, tailored to the type of audience we were presenting the matter to.
Table 3.10: Summary of All Security Awareness Seminars and Short Courses

<table>
<thead>
<tr>
<th>Activity</th>
<th>Venue</th>
<th>Duration (Days)</th>
<th>Audience</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seminar1</td>
<td>Court Yard</td>
<td>1</td>
<td>IT Practitioners</td>
<td>65</td>
</tr>
<tr>
<td>Seminar2</td>
<td>UDSM</td>
<td>½</td>
<td>UDSM Staff</td>
<td>42</td>
</tr>
<tr>
<td>Seminar3</td>
<td>Royal Palm</td>
<td>1</td>
<td>CEOs</td>
<td>61</td>
</tr>
<tr>
<td>Seminar4</td>
<td>UCLAS</td>
<td>½</td>
<td>Staff +Students</td>
<td>31</td>
</tr>
<tr>
<td>Seminar5</td>
<td>SUZA</td>
<td>1</td>
<td>Staff +Students</td>
<td>41</td>
</tr>
<tr>
<td>Seminar6</td>
<td>AIA</td>
<td>1</td>
<td>Staff +Students</td>
<td>400</td>
</tr>
<tr>
<td>Seminar7</td>
<td>DICC</td>
<td>1</td>
<td>Local +Internationals</td>
<td>50</td>
</tr>
<tr>
<td>Seminar8</td>
<td>DICC</td>
<td>5</td>
<td>IT Practitioners</td>
<td>40</td>
</tr>
<tr>
<td>Seminar9</td>
<td>GDLC</td>
<td>1</td>
<td>Civil Servants</td>
<td>14</td>
</tr>
<tr>
<td>Seminar10</td>
<td>COSTECH</td>
<td>1</td>
<td>IT Practitioners</td>
<td>50</td>
</tr>
<tr>
<td>Course1</td>
<td>UDSM</td>
<td>2</td>
<td>Students</td>
<td>214</td>
</tr>
<tr>
<td>Course2</td>
<td>UDSM</td>
<td>1</td>
<td>Students</td>
<td>148</td>
</tr>
<tr>
<td>Course3</td>
<td>UDSM</td>
<td>1</td>
<td>Students</td>
<td>178</td>
</tr>
<tr>
<td>Course4</td>
<td>UCC-Arusha</td>
<td>1</td>
<td>Students</td>
<td>39</td>
</tr>
</tbody>
</table>

Key:  
GDLC – Global Development Learning Center – Tanzania  
COSTECH – Commission for Science and Technology – Tanzania  
DICC – Dar es Salaam International Conference Centre  
AIA – Arusha Institute of Accountancy  
UCLAS – University College of Lands and Architectural Studies  
UDSM – University of Dar es Salaam  
UCC – University Computing Centre  
SUZA – State University of Zanzibar

From Table 3.10 it can be noted that at least 1300 people have attended one or more of our security seminars and short courses. The figure does not include those who have read our security articles in the periodicals discussed earlier in this chapter. If all these are going to spread a word on security in their organisations, certainly its impact will be enormous.
3.11 Chapter Summary

In this chapter we have attempted to give details of the entire research process. We have presented and described the two research cycles and gave outputs for each of the cycles. Validations of the first research cycle have also been demonstrated in this chapter. Then we presented the perceived impacts of our security awareness seminars and short courses in Tanzania.
Chapter 4

EMPIRICAL ANALYSIS OF SECURITY SURVEY

In this chapter we present and discuss empirical analysis of the security survey that was carried out to track and investigate information security practices in organisations. We describe the whole process from design, distribution, management and analysis of the questionnaires. Then we present results from the questionnaires and discuss reflections made from these results. Finally, we briefly discuss the key findings from the Deloitte (2005) global security survey in comparison with the key elements of the proposed DAISA approach.

4.1 Purpose of the Security Survey

To understand and address information security aspects in organisations, one should first properly understand how security is being practiced in organisations under investigation. The purpose of this empirical information security survey, thus, was to investigate and track security practices within organisations in Tanzania. Results from this survey were meant to complement other findings gathered from different methods used for data collection (such as interviews, seminars and courses, comments from conferences, and literature review) in setting up the basis for developing an effective organisational security awareness approach. On tracking security practices in organisations, different questions in a questionnaire were aimed at
accomplishing different objectives. The specific objectives of the survey were to track and investigate:

1) How often do respondents access computers or network
2) Where do they access computers
3) How do they value information assets
4) Level of respondents security awareness
5) Composition of respondents
6) Interconnectivity status
7) Information security practices at workplace
8) Managements support/commitment to security initiatives
9) Experience of respondents on security attacks in their organisations
10) Whether security awareness at workplaces was necessary at the moment
11) Demographic attributes of the respondents

All 44 questions in the questionnaire contributed towards accomplishing these 11 specific objectives. Table 4.1 illustrates the matching between questions in the questionnaire vis-à-vis specific objectives. As it may be noted from Table 4.1 about 16 out of 44 questions in the questionnaire were specifically targeting information security practices at workplace whereas 13 questions were meant to assess the level of security awareness of the respondents. This was deliberately done since the specific objectives 4 and 7 were paramount to fulfilling the purpose of the survey and, eventually, guiding us in developing the awareness approach. The two objectives were closely related to each other and to the purpose of the survey.
Table 4.1: Questionnaire’s Questions vis-à-vis Specific Objectives

<table>
<thead>
<tr>
<th>S/N</th>
<th>Specific Objectives</th>
<th>Corresponding Questions #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>How often do respondents access computers or network</td>
<td>1</td>
</tr>
<tr>
<td>2.</td>
<td>Where do they access computers</td>
<td>2</td>
</tr>
<tr>
<td>3.</td>
<td>How do they value information assets</td>
<td>3, 4</td>
</tr>
<tr>
<td>4.</td>
<td>Level of respondents security awareness</td>
<td>5, 6, 7, 8, 9, 10, 28, 31, 34, 37, 38, 41, 42</td>
</tr>
<tr>
<td>5.</td>
<td>Composition of respondents</td>
<td>11</td>
</tr>
<tr>
<td>6.</td>
<td>Interconnectivity status in organisations</td>
<td>12, 13</td>
</tr>
<tr>
<td>7.</td>
<td>Information security practices at workplace</td>
<td>14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 25, 27, 32, 33, 39, 40</td>
</tr>
<tr>
<td>8.</td>
<td>Managements support/commitment to security initiatives</td>
<td>26</td>
</tr>
<tr>
<td>9.</td>
<td>Experience of respondents on security attacks in their organisations</td>
<td>29, 30</td>
</tr>
<tr>
<td>10.</td>
<td>Whether security awareness at workplaces was necessary at the moment</td>
<td>35, 36</td>
</tr>
<tr>
<td>11.</td>
<td>Demographic attributes of the respondents</td>
<td>43, 44</td>
</tr>
</tbody>
</table>

4.2 Questionnaire Design and Management

In order to capture the requirements for security awareness and learn more on existing security practices in organisations we designed, distributed and collected questionnaires.

4.2.1 Questionnaire Design

Questionnaires were specifically designed to assess and track trends in today’s information security awareness and practices at workplaces. We included both closed and open-ended questions depending on what we wanted to infer out of
that particular question. Each questionnaire had a total of 44 questions. We did not disclose the actual aim of the questionnaires to the respondents except that it was a confidential survey to collect data for research purposes only. Concealment of the aim of the questionnaire was intentionally done to avoid leading respondents on how or what to answer. Questionnaires were filled-in anonymously in that there were no room to disclose personal particulars or identity of the respondent. A sample of the questionnaires is attached as Appendix D. The mode of distribution was one questionnaire per organisation. Thus, the target was to carry out our study in 100 different organisations. These include government agencies, non-governmental and private organisations, and academic or learning institutions ranging from small to large organisations.

4.2.2 Questionnaire Distribution
A total of 100 questionnaires were reproduced and distributed. We distributed 20 questionnaires in Zanzibar, another 20 questionnaires in Arusha and the remaining 60 copies were distributed in Dar es Salaam. These are the regions that were considered to have higher density of computer users in Tanzania. Only 20 out of 100 questionnaires were distributed to people who had attended at least one of our seminars or short courses before. The remaining 80 questionnaires were distributed to those who had not attended our seminars or courses before. Table 4.2 summarises distributions of questionnaires.
Table 4.2: Summary of Questionnaires Distributions

<table>
<thead>
<tr>
<th>Location/Area</th>
<th>No. of Questionnaires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zanzibar</td>
<td>20</td>
</tr>
<tr>
<td>Arusha</td>
<td>20</td>
</tr>
<tr>
<td>Dar es Salaam</td>
<td>60</td>
</tr>
</tbody>
</table>

Since it was not practicable to distribute questionnaires throughout the country given limited time and resources, we had to select the three regions as shown in Table 4.2. The three were chosen based on merits that they had relatively higher degree of ICT usage compared to other regions in the country.

4.2.3 Questionnaire Collection

Collection of the questionnaires back from the respondents was the most difficult exercise. We only managed to collect back 64 questionnaires out of 100 that were distributed earlier. This means only 64% of the questionnaires were collected back duly filled. Only 9 questionnaires were collected from Zanzibar out of the 20 that were distributed in the area. This is obviously less than 50% return of the questionnaires. From Arusha we managed to get back 11 questionnaires out of 20 that were distributed in there. At least this is slightly higher than 50% return. Table 4.3 gives a summary of collection of the questionnaires against distributions. From Dar es Salaam we managed to collect back 44 questionnaires duly filled out of 60 that were distributed in the area. This was about 73.3% return.
Table 4.3: Summary of Questionnaires Collection

<table>
<thead>
<tr>
<th>Location/Area</th>
<th>Distributed</th>
<th>Collected</th>
<th>Percentage Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zanzibar</td>
<td>20</td>
<td>9</td>
<td>45%</td>
</tr>
<tr>
<td>Arusha</td>
<td>20</td>
<td>11</td>
<td>55%</td>
</tr>
<tr>
<td>Dar es Salaam</td>
<td>60</td>
<td>44</td>
<td>73.3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
<td><strong>64</strong></td>
<td><strong>64%</strong></td>
</tr>
</tbody>
</table>

Only 14 questionnaires were collected from the stratum of those who had attended our seminars and courses out of the 20 distributed to them. This means that 50 questionnaires were collected back from the second stratum out of the eighty that were distributed.

Organisations that did not return our questionnaires back gave various ‘good’ reasons such as it has been misplaced so we are sorry we cannot locate it. Others said someone with our questionnaire was away on official business while others said someone went on leave without handing over our questionnaires. There were many other reasons but of course all of them trying to justify the loss of our questionnaires.

4.3 Sampling Techniques Used

Before selecting the sampling techniques to apply for our survey we went through various sampling techniques Levy and Lemeshow (1999) at our disposal. In the process we managed to go through at least 10 different statistical sampling techniques. These include the following:

1) Random sampling
2) Simple random sampling
3) Stratified sampling
Since it is not the aim of this thesis to deal with sampling techniques, we shall limit ourselves to the two techniques that were used for this work. For sampling our population we applied both *Simple Random Sampling* and *Stratified Random Sampling*. Both definitions are based on Levy and Lemeshow (1999).

**Simple Random Sampling** – Refers to any sort of sampling whereby, before selection of the sample, each member of the population has a calculable and non-zero chance of selection. In addition, each member of the population has the same chance of selection, and the relative chance of selection of any two members of the population is not affected by the knowledge of whether a third member has or has not been selected.

**Stratified Random Sampling** – Here the population is divided into non-overlapping groups, called *Strata*, according to some characteristics. Samples are then drawn from each stratum separately and results pooled.

When distributing the questionnaires we applied these two techniques in that, first any individual in the organisation had equal chance of getting and filling-in a questionnaire, meaning simple random sampling. Secondly, we divided
our population into two non-overlapping strata, that is, those who had earlier attended our seminars or short courses; and the other stratum were those who had not attended to any of those events, that means stratified random sampling. The questionnaires were the same for the two strata.

4.4 Analysis of Questionnaires
To analyse our questionnaires we applied one of the famous statistical data analysis software. This is called Statistical Package for Social Scientists (SPSS) Version 12. The full results of the analysis from the SPSS engine are discussed in the subsequent section. Excerpts from the SPSS engine are presented in tabular format and discussed thereafter for the purpose of clarity. Despite the many statistical ratios offered by SPSS we were only interested in frequency tables. The questionnaires results are presented and discussed in Table 4.4 through Table 4.46 in the subsequent section.

4.5 Discussion and Interpretation of the Results
Our discussions on these results begins with comparison of responses from the two strata i.e. responses from those who had attended our seminars or courses vis-à-vis those who had not. It was observed that there was no significant difference in responses from the two strata. The only difference was on the question of whether someone had ever attended security training before or not. We believe that was because of the nature of the questions on the questionnaires. The questionnaire was aimed at tracking what was going on in practice in organisations. In that case, the question of whether one had
attended a security seminar or not could not make a difference unless his/her organisation had significantly changed in security terms as a result of that seminar. It should be noted that the number of respondents is 64, thus this is our basis. In this case from now on we shall be referring to the percentages only without mentioning the number of respondents for simplicity reasons. Following below are detailed discussions of the results in Table 4.4 through Table 4.46.

<table>
<thead>
<tr>
<th>Table 4.4: How often do you access a computer and/or network?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
</tr>
<tr>
<td>Valid On daily basis</td>
</tr>
<tr>
<td>At least once a week</td>
</tr>
<tr>
<td>At least once a month</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Nearly 86% of respondents were accessing certain information assets on daily basis as indicated in Table 4.4. On the other hand, that was a good indication on our side that information gathered from their responses was from the very people of our target. Only less than 5% of respondents were accessing information assets at least once a month.
Table 4.5: Where do you access a computer?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>At work only</td>
<td>32</td>
<td>50.0</td>
<td>50.0</td>
<td>50.0</td>
</tr>
<tr>
<td>Both at work and home</td>
<td>23</td>
<td>35.9</td>
<td>35.9</td>
<td>85.9</td>
</tr>
<tr>
<td>At internet Cafe</td>
<td>7</td>
<td>10.9</td>
<td>10.9</td>
<td>96.9</td>
</tr>
<tr>
<td>Other, Specify</td>
<td>2</td>
<td>3.1</td>
<td>3.1</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

From Table 4.5 fifty percent of respondents were accessing computers at work only whereas 35.9% were accessing computers both at work and at home as well. This was an indication that a good number of people can afford to buy computers for their home use. This might partly be results of exemption of the import duty on computers from abroad into the country as discussed in Chapter 1. Alternatively, it may be that many people in Tanzania have understood the importance of using computers in a way that they are even sacrificing a little they have to buy computers for their own and their families. Another important inference drawn from this finding is that it prompts for the need to address security requirements for kids and teenagers with computers at home now. Teenagers have their own, and sometimes specific, ambitions when using computers and the Internet in particular. If teenagers are not properly guided, especially, on ethical use of computer systems it may turn into a society’s problem in future. Nonetheless, aspects of security for kids and teenagers are not fully addressed by this thesis, only that it is recommended as part of future research.
Table 4.6: Do you think data and information in a computer are important assets?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Interestingly, from Table 4.6 all of respondents acknowledged that data and information in a computer were important assets.

Table 4.7: Do you think it is worth to protect data and information in computer systems?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>57</td>
<td>89.1</td>
<td>89.1</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>5</td>
<td>7.8</td>
<td>7.8</td>
</tr>
<tr>
<td></td>
<td>Not sure</td>
<td>1</td>
<td>1.6</td>
<td>1.6</td>
</tr>
<tr>
<td></td>
<td>Other, Specify...</td>
<td>1</td>
<td>1.6</td>
<td>1.6</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Conversely, from Table 4.7 only 89.1% of respondents thought it was worth to protect data and information in computer systems. One respondent argued that the question of whether to protect or not depends on what information is stored in that computer. The argument, however, seems to contradict his response in Table 4.6 where he said data and information in a computer were important assets. In our view, every data stored in a computer system deserves some sort of protection proportional to its value. It is, therefore, upon the owner of the data to decide on the required protection.
Table 4.8: Have you ever heard/read anything about information security?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>52</td>
<td>81.3</td>
<td>81.3</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>11</td>
<td>17.2</td>
<td>98.4</td>
</tr>
<tr>
<td></td>
<td>Other, Specify...</td>
<td>1</td>
<td>1.6</td>
<td>1.6</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

As much as 81.3% of respondents had heard or at least read something about information security, Table 4.8, whereas 17.2% had no idea about it. One respondent commented that although she had not formally heard or read about it, she thought it was all about protecting information flowing thought a computer network. That response, however, suggests that she knew it, and all she needed was guidelines on how to properly do that protection.

Table 4.9: If you have responded, "Yes" to question #5 above please mention through which media?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Newsletter/Journal</td>
<td>16</td>
<td>25.0</td>
<td>25.0</td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td>19</td>
<td>29.7</td>
<td>54.7</td>
</tr>
<tr>
<td></td>
<td>Radio/TV</td>
<td>3</td>
<td>4.7</td>
<td>59.4</td>
</tr>
<tr>
<td></td>
<td>Other specify</td>
<td>14</td>
<td>21.9</td>
<td>81.3</td>
</tr>
<tr>
<td></td>
<td>Not applicable</td>
<td>12</td>
<td>18.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Interestingly from Table 4.9 one-fourth of respondents read about security in Newsletter. Nearly 22% heard about security from the seminar as well as reading about it in Newsletters, under other specify. Even though not
explicitly specified, we presume the Newsletters referred to are ones prepared by the University of Dar es Salaam Computing Centre discussed in Chapter 3 and Chapter 5.

Table 4.10: Do you know what information security is all about?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>46</td>
<td>71.9</td>
<td>71.9</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>11</td>
<td>17.2</td>
<td>89.1</td>
</tr>
<tr>
<td></td>
<td>Not sure</td>
<td>7</td>
<td>10.9</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Though many (81.3% in Table 4.8) had heard or read about information security, in Table 4.10 only 71.9% of respondents knew exactly what it was all about. This implies that hearing or reading about security is one thing, and knowing it is quite another.

Table 4.11: How do you view/perceive information security?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>It is a technical issue</td>
<td>21</td>
<td>32.8</td>
<td>32.8</td>
</tr>
<tr>
<td></td>
<td>It is a non-technical issue</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
</tr>
<tr>
<td></td>
<td>It is both technical and non-technical issue</td>
<td>29</td>
<td>45.3</td>
<td>45.3</td>
</tr>
<tr>
<td>Not sure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>
From Table 4.11 fairly 32.8% of respondents perceived information security as a technical issues whereas 45.3% viewed security as both a technical and non-technical issue. About 17% were unsure on the real nature of information security.

Table 4.12: Ever you attended to any information security training?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>23</td>
<td>35.9</td>
<td>35.9</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>41</td>
<td>64.1</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Impressively, from Table 4.12 nearly 36% of respondents had attended to some sort of Information security training. In the meantime, 64.1% had not attended to any information security training.

Table 4.13: If you have responded, "Yes" to question # 9 above please mention which training?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Seminar/Workshop</td>
<td>10</td>
<td>15.6</td>
<td>15.6</td>
</tr>
<tr>
<td>Academic program</td>
<td>10</td>
<td>15.6</td>
<td>15.6</td>
<td>31.3</td>
</tr>
<tr>
<td>Other, Specify..... ..</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
<td>35.9</td>
</tr>
<tr>
<td>Not applicable</td>
<td>41</td>
<td>64.1</td>
<td>64.1</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

From Table 4.13 about 15.6 % of respondents had attended security seminars, and the same proportion of respondents attended security as academic
programs. The latter might have attended security education abroad. This shows that many are yet to hear something on information security.

Table 4.14: Which category is your organisation?

<table>
<thead>
<tr>
<th>Category</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Private/NGO</td>
<td>27</td>
<td>42.2</td>
<td>42.2</td>
<td>42.2</td>
</tr>
<tr>
<td>Governmental</td>
<td>16</td>
<td>25.0</td>
<td>25.0</td>
<td>67.2</td>
</tr>
<tr>
<td>Academic/Learning Institution</td>
<td>21</td>
<td>32.8</td>
<td>32.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

As much as 42.2% of respondents were working with either private companies or non-governmental organisations whereas one-fourth of respondents were working with either the central government (of Tanzania) or other government agencies. From Table 4.14 the remaining 32.8% were working with academic institutions. In our view, that was a good mix in that to properly address security issues there need to be a combined support and collaboration of the industry, academia and government.

Table 4.15: Does your organisation have a Local Area Network (LAN)?

<table>
<thead>
<tr>
<th>Category</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>57</td>
<td>89.1</td>
<td>89.1</td>
<td>89.1</td>
</tr>
<tr>
<td>No</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
<td>93.8</td>
</tr>
<tr>
<td>Not sure</td>
<td>4</td>
<td>6.3</td>
<td>6.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
From Table 4.15 it can be seen that 89.1% of respondents had their organisations installed with Local Area Networks (LAN). This means that sharing of information over the network was possible in those organisations posing more security risks to the networked information resources if not adequately protected.

Table 4.16: Does your organisation have at least one computer with access to the Internet?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>61</td>
<td>95.3</td>
<td>95.3</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Nearly all (95.3%) of respondents had their organisations linked to the Internet, Table 4.16. Much as connection to the Internet is a great thing, it also increases exposure of the organisation’s information assets to global threats. This is the fact that all organisations connected to the Internet have to be aware of.

Table 4.17: Does your organisation have a written Information Security Policy?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>16</td>
<td>25.0</td>
<td>25.0</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>23</td>
<td>35.9</td>
<td>60.9</td>
</tr>
<tr>
<td></td>
<td>Not Sure</td>
<td>25</td>
<td>39.1</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

A quarter of respondents had their organisations with written information security policies. Table 4.17 indicates that the remaining 75% of respondents
either did not have it or if they had one, then it was not known to the respondents. In either case, it means one and the same thing in practice since a security policy was supposed to be known to all employees.

Table 4.18: If you have responded, "Yes" to question #14 above are all employees aware of the policy?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>10</td>
<td>15.6</td>
<td>15.6</td>
<td>15.6</td>
</tr>
<tr>
<td>No</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
<td>20.3</td>
</tr>
<tr>
<td>Not sure</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
<td>25.0</td>
</tr>
<tr>
<td>Not applicable</td>
<td>48</td>
<td>75.0</td>
<td>75.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

Surprisingly, from Table 4.18 less than half of respondents who had written security policies had all employees in their organisations aware of the policies. This means that even those few with written information security policies in place, the policies were not effectively communicated to all staffs. Effective communication of a security policy to all employees is critically important for it to be enforceable.
Table 4.19: If you have responded, "Yes" to question #15 above how is the policy communicated to employees?

<table>
<thead>
<tr>
<th>Valid</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>During orientation program</td>
<td>6</td>
<td>9.4</td>
<td>9.4</td>
<td>9.4</td>
</tr>
<tr>
<td>Given as part of one's Terms of Reference (TOR)</td>
<td>2</td>
<td>3.1</td>
<td>3.1</td>
<td>12.5</td>
</tr>
<tr>
<td>Posted on the staff notice board</td>
<td>2</td>
<td>3.1</td>
<td>3.1</td>
<td>15.6</td>
</tr>
<tr>
<td>Not applicable</td>
<td>54</td>
<td>84.4</td>
<td>84.4</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

Various methods were applied to communicate information security policies in those few organisations that had the policies. From Table 4.19 such methods include highlighting on the policy during staff’s orientation programs, given to staffs as part of their Terms of References (TOR) and posting the policy on staff notice boards for everybody to read.

Table 4.20: Does your organisation have any formal and regular information security awareness training program?

<table>
<thead>
<tr>
<th>Valid</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>11</td>
<td>17.2</td>
<td>17.2</td>
<td>17.2</td>
</tr>
<tr>
<td>No</td>
<td>38</td>
<td>59.4</td>
<td>59.4</td>
<td>76.6</td>
</tr>
<tr>
<td>Not sure</td>
<td>15</td>
<td>23.4</td>
<td>23.4</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
Interestingly, from Table 4.20 only 17.2% of respondents had their organisations with formal and regular information security awareness programs. This on the other hand means that the remaining more than 80% of the organisations studied did not have security awareness programs for its employees.

Table 4.21: If you have responded "Yes" to question #17 above whom does the program target?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid All employees</td>
<td>6</td>
<td>9.4</td>
<td>9.4</td>
<td>9.4</td>
</tr>
<tr>
<td>Only IT staff</td>
<td>5</td>
<td>7.8</td>
<td>7.8</td>
<td>17.2</td>
</tr>
<tr>
<td>Not applicable</td>
<td>53</td>
<td>82.8</td>
<td>82.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Even for those organisations that had security awareness programs, about 50% had their awareness programs targeting all employees. The rest had their security programs dedicated to IT staffs only, Table 4.21.

Table 4.22: If you have responded, "Yes" to question #17 above how often is the program offered?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid At least once a month</td>
<td>2</td>
<td>3.1</td>
<td>3.1</td>
<td>3.1</td>
</tr>
<tr>
<td>Yearly</td>
<td>4</td>
<td>6.3</td>
<td>6.3</td>
<td>9.4</td>
</tr>
<tr>
<td>Not sure</td>
<td>5</td>
<td>7.8</td>
<td>7.8</td>
<td>17.2</td>
</tr>
<tr>
<td>Not applicable</td>
<td>53</td>
<td>82.8</td>
<td>82.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>
From Table 4.22 nearly half of respondents whose organisations had security awareness programs were even not sure of how frequent were such programs offered. The rest had it once a year and just 2 respondents had it offered at least once a month.

![Table 4.23: Does your organisation have a computer/network security unit?](image)

Another interesting result in Table 4.23 was that only 34.4% of respondents had their organisations with a special unit for computer or network security.

![Table 4.24: Does your organisation have a computer incident response plan?](image)

Surprisingly, from Table 4.24 only 21.9% of respondents had their organisations with computer incident response plan. This means that in the rest of the organisations not only that employees do not know where to report suspicious security incidents but also that apparently those organisations start planning on how to deal with a particular security incident right after
happening. We do not see that as the best practice, especially, in organisations that are dependent on computer systems in their day-to-day business operations. Each organisation need to have a plan beforehand that guides its responses to different information security threats and vulnerabilities.

**Table 4.25: Does your organisation have a computer disaster recovery plan?**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>16</td>
<td>25.0</td>
<td>25.0</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>19</td>
<td>29.7</td>
<td>54.7</td>
</tr>
<tr>
<td></td>
<td>Not sure</td>
<td>29</td>
<td>45.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Likewise, from Table 4.25 only one-fourth of respondents had their organisations equipped with computer disaster recovery plans. That was really alarming situation should a very serious disaster incident such a lightening, floods, earthquake and the like occur to the rest of the organisations.

**Table 4.26: Does your organisation have well-documented Backup Procedure for its data?**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>23</td>
<td>35.9</td>
<td>35.9</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>17</td>
<td>26.6</td>
<td>62.5</td>
</tr>
<tr>
<td></td>
<td>Not sure</td>
<td>24</td>
<td>37.5</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Similar to the previous two result tables, Table 4.26 indicates that only 35.9% of respondents had well-documented data backup procedures. Again, certainly that was not a good indication, especially, for organisations that hope to
leapfrog the many steps of ICT developments and take on the state-of-the-art high tech. We can correctly guess that the majority of respondents whose organisations had proper backup procedures were from banks and other financial institutions. This is due to the fact that banks in Tanzania were relatively ahead of other institutions when it comes to information security.

**Table 4.27:** Does your organisation have a budget for protecting its information assets?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>25</td>
<td>39.1</td>
<td>39.1</td>
<td>39.1</td>
</tr>
<tr>
<td>No</td>
<td>13</td>
<td>20.3</td>
<td>20.3</td>
<td>59.4</td>
</tr>
<tr>
<td>Not sure</td>
<td>26</td>
<td>40.6</td>
<td>40.6</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Only 39% of respondents had their organisations setting aside a special budget for security of its information assets, Table 4.27.

**Table 4.28:** If you have responded, "Yes" to question #24 above does the budget also cover training of employees in security awareness?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>14</td>
<td>21.9</td>
<td>21.9</td>
<td>21.9</td>
</tr>
<tr>
<td>No</td>
<td>11</td>
<td>17.2</td>
<td>17.2</td>
<td>39.1</td>
</tr>
<tr>
<td>Not applicable</td>
<td>39</td>
<td>60.9</td>
<td>60.9</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Of those organisations that had budgets for information security Table 4.28, only about half of them had their budgets including promotion of security.
awareness in their organisations. It was commented that a lion share of the security budget was dedicated on buying technical security tools and mechanisms.

**Table 4.29**: Is the management of your organisation supportive/committed to information security?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Yes</th>
<th>No</th>
<th>Not sure</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>26</td>
<td>9</td>
<td>29</td>
<td>64</td>
</tr>
<tr>
<td>Percent</td>
<td>40.6</td>
<td>14.1</td>
<td>45.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Valid Percent</td>
<td>40.6</td>
<td>14.1</td>
<td>45.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Cumulative Percent</td>
<td>40.6</td>
<td>54.7</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

From Table 4.29 about 40 percent of respondents acknowledged that their managements were supporting security initiatives in their respective organisations. Commitment of the top management to security initiatives is pivotal to the success of security initiatives in organisations.

**Table 4.30**: Is security awareness training (formal or informal) conducted in your organisation prior to users receiving access to an IT application or IT services?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Yes</th>
<th>No</th>
<th>Not sure</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>20</td>
<td>32</td>
<td>12</td>
<td>64</td>
</tr>
<tr>
<td>Percent</td>
<td>31.3</td>
<td>50.0</td>
<td>18.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Valid Percent</td>
<td>31.3</td>
<td>50.0</td>
<td>18.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Cumulative Percent</td>
<td>31.3</td>
<td>81.3</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

Security awareness training (formal or informal) was not conducted to staff prior to granting them access to IT resources except in only 31.3% of respondents’ organisations, Table 4.30.
Table 4.31: Are you aware of any threats, risks and vulnerabilities to your organisation's information assets?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>67.2</td>
<td>67.2</td>
</tr>
<tr>
<td>No</td>
<td>18.8</td>
<td>85.9</td>
</tr>
<tr>
<td>Not sure</td>
<td>14.1</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

At least 67% of respondents in Table 4.31 were aware of risks, threats and vulnerabilities to information assets. The rest of the respondents were not even aware of security risks and threats out there. These responses show that many people were aware of the threats and vulnerabilities to the information assets, what they were lacking though was appropriate knowledge on how to deal with them. That stands to reason for the need of an approach such as DAISA that is described in Chapter 6.

Table 4.32: Have you ever encountered computer virus attack in your organisation?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>75.0</td>
<td>75.0</td>
</tr>
<tr>
<td>No</td>
<td>20.3</td>
<td>95.3</td>
</tr>
<tr>
<td>Not sure</td>
<td>4.7</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Three quarters of respondents in Table 4.32 had encountered computer virus at some point in their day-to-day operations with computer systems. Computer
virus and other malicious codes were cited by respondents as the most common security threat in their organisations.

**Table 4.33**: Had your organisation's computer system ever been attacked or compromised?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>29</td>
<td>45.3</td>
<td>45.3</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>14</td>
<td>21.9</td>
<td>67.2</td>
</tr>
<tr>
<td></td>
<td>Not sure</td>
<td>21</td>
<td>32.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

When prompted for security attack experiences in their organisations, only 45.3% acknowledged that their computer systems had been compromised at some points. In Table 4.33, the rest of the respondents did not disclose their attack experiences. That does not necessarily mean that they had never been attacked; it may also mean that those respondents were not allowed to disclose such attacks history information to the outsiders.

**Table 4.34**: Do you think information security awareness is a problem/challenge that needs to be addressed in your organisation?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>54</td>
<td>84.4</td>
<td>84.4</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>5</td>
<td>7.8</td>
<td>92.2</td>
</tr>
<tr>
<td></td>
<td>Not sure</td>
<td>5</td>
<td>7.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>64</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
Interestingly, 84.4% of respondents viewed security awareness as a challenge that needed to be addressed in organisations. Responses in Table 4.34 signify the necessity for establishing security awareness programs at workplaces.

Table 4.35: Are you aware of any laws/policies governing information security practices at a country level (Tanzania)?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid No</td>
<td>37</td>
<td>57.8</td>
<td>57.8</td>
<td>57.8</td>
</tr>
<tr>
<td>Not sure</td>
<td>27</td>
<td>42.2</td>
<td>42.2</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Perhaps as was expected, none of respondents were aware of any country-level policies on information security in Tanzania, Table 4.35. That calls for the need to establish the country security code of practices or at least to adopt and customise existing international security codes of practices. The country-level security guidelines (if established) would bring uniformity in security practices in organisations. The move shall make it easier even for the e-government initiatives to take place with many entities in the country on board.

Table 4.36: Are you aware of any academic institution or any other learning institution teaching information security courses in Tanzania?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>20</td>
<td>31.3</td>
<td>31.3</td>
<td>31.3</td>
</tr>
<tr>
<td>No</td>
<td>34</td>
<td>53.1</td>
<td>53.1</td>
<td>84.4</td>
</tr>
<tr>
<td>Not sure</td>
<td>10</td>
<td>15.6</td>
<td>15.6</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Surprisingly, 31.3 percent of respondents said they were aware of academic institutions in Tanzania that were offering information security courses, Table 4.36. From our experience gained in the course of this research, as of year 2005 there were none of such institutions. However, it might be that respondents were referring to the security short courses we offered at the University of Dar es Salaam as discussed in Chapter 3.

**Table 4.37:** Do you think there is a need to establish information security awareness programs at a workplace?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>60</td>
<td>93.8</td>
</tr>
<tr>
<td>No</td>
<td>1</td>
<td>1.6</td>
<td>1.6</td>
</tr>
<tr>
<td>Not sure</td>
<td>3</td>
<td>4.7</td>
<td>4.7</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Nearly all (93.8%) of respondents conceded that there was a need for establishing information security awareness programs at workplaces. In Table 4.37, only 3 respondents were not sure about it and one respondent said there was no need.

**Table 4.38:** If you responded “Yes” to question #35 above, whom do you think need to be trained in information security awareness at your organisation?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>IT staff only</td>
<td>6</td>
<td>9.4</td>
</tr>
<tr>
<td></td>
<td>All employees</td>
<td>54</td>
<td>84.4</td>
</tr>
<tr>
<td></td>
<td>Not applicable</td>
<td>4</td>
<td>6.3</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Of those supporting establishment of security awareness programs at workplaces, 93.8% said the program should target all employees. In Table 4.38, only 9.4% of respondents said awareness programs should target IT staff only. In practice, security awareness programs should target all employees in an organisation including the top management. Modes of delivery may differ from one category of staff to another, but every one has a role to play in making security awareness a success in organisation.

Table 4.39: Do you think there are any threats/risks to your data/information in a computer when accessing the Internet?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>52</td>
<td>81.3</td>
<td>81.3</td>
<td>81.3</td>
</tr>
<tr>
<td>Valid No</td>
<td>4</td>
<td>6.3</td>
<td>6.3</td>
<td>87.5</td>
</tr>
<tr>
<td>Valid Not Sure</td>
<td>8</td>
<td>12.5</td>
<td>12.5</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

As much as 81.3% of respondents were aware of the risks to data in their computer systems when accessing the Internet. However, in Table 4.39 about 12.5% of respondents were completely not aware of risks they were facing on accessing the Internet.
Table 4.40: Where do you think an attack or compromise to your data/information in a computer may come from?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Within the organisation</td>
<td>2</td>
<td>3.1</td>
<td>3.1</td>
<td>3.1</td>
</tr>
<tr>
<td>Outside the organisation</td>
<td>7</td>
<td>10.9</td>
<td>10.9</td>
<td>14.1</td>
</tr>
<tr>
<td>Both within and outside the organisation</td>
<td>49</td>
<td>76.6</td>
<td>76.6</td>
<td>90.6</td>
</tr>
<tr>
<td>Not sure</td>
<td>6</td>
<td>9.4</td>
<td>9.4</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Another interesting result was in Table 4.40 where 90.6% of respondents said they knew that attacks to their corporate information assets might emanate from within as well as outside their organisations. As discussed in Chapter 2, this is what happens in practice.

Table 4.41: Are all computers in your organisation installed with antivirus software?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>38</td>
<td>59.4</td>
<td>59.4</td>
<td>59.4</td>
</tr>
<tr>
<td>No</td>
<td>10</td>
<td>15.6</td>
<td>15.6</td>
<td>75.0</td>
</tr>
<tr>
<td>Not sure</td>
<td>16</td>
<td>25.0</td>
<td>25.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

From Table 4.41, only 59.4% of respondents had all computers in their organisations installed with antivirus software. This means that the remaining more than 40% were either unsure or antivirus software not installed in all of their computers. Organisations that have their computers connected over Local Area Networks (LAN) should have all of their computers installed with
antivirus short of which they run a risk of viruses propagating over the network.

**Table 4.42**: If you have responded, "Yes" to question #39 above, is the antivirus software updated on regular basis?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>26</td>
<td>40.6</td>
<td>40.6</td>
<td>40.6</td>
</tr>
<tr>
<td>Valid No</td>
<td>5</td>
<td>7.8</td>
<td>7.8</td>
<td>48.4</td>
</tr>
<tr>
<td>Valid Not sure</td>
<td>7</td>
<td>10.9</td>
<td>10.9</td>
<td>59.4</td>
</tr>
<tr>
<td>Valid Not applicable</td>
<td>26</td>
<td>40.6</td>
<td>40.6</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

From Table 4.42 even those who had all of their computers installed with antivirus software, only 40.6% had it updated regularly. Perhaps it is important to point out that having antivirus installed in ones computer is one thing and updating it regularly is another thing. New viruses and other malicious codes such as Worms and Trojan horses are discovered nearly everyday. It is, therefore, recommended to configure the antivirus software to automatically update itself as soon as you switch on your computer and given that new antivirus updates have been released by the software manufacturer.

**Table 4.43**: Are you aware of "social engineering" tricks?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>16</td>
<td>25.0</td>
<td>25.0</td>
<td>25.0</td>
</tr>
<tr>
<td>Valid No</td>
<td>44</td>
<td>68.8</td>
<td>68.8</td>
<td>93.8</td>
</tr>
<tr>
<td>Valid Not sure</td>
<td>4</td>
<td>6.3</td>
<td>6.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
Alas, only one-fourth of respondents were aware of the deadly social engineering tricks. Others in Table 4.43, about 75% of respondents were completely unaware of such tricks. Social engineering tricks, essentially, refers to the techniques of circumventing technological security measures by manipulating people to disclose crucial authentication information. There are many different ways in which social engineering is done from telephone calls to email and the like.

<table>
<thead>
<tr>
<th>Table 4.44: Do you use Internet and/or E-mail regularly?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frequency</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Valid Yes 62</td>
</tr>
<tr>
<td>No 2</td>
</tr>
<tr>
<td>Total 64</td>
</tr>
</tbody>
</table>

Nearly all (96.9%) of respondents were frequent users of email and Internet. In Table 4.44 only 3.1% of respondents were not regular users of email and Internet.

<table>
<thead>
<tr>
<th>Table 4.45: Gender</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frequency</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Valid Male 40</td>
</tr>
<tr>
<td>Female 24</td>
</tr>
<tr>
<td>Total 64</td>
</tr>
</tbody>
</table>

Gender proportions of respondents were at 62.5% males and 37.5% females, Table 4.45. Given the fact on the ground, we can say that was relatively a fairly balanced gender distribution. The argument is based on the fact that at
the time of this research the IT industry in Tanzania was mainly dominated by males compared to female practitioners in the field. Generally, there were fewer female students in computer science and engineering fields than males. In other fields of study, however, the proportions of the two genders were relatively balanced.

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-40 years</td>
<td>51</td>
<td>79.7</td>
<td>79.7</td>
<td>79.7</td>
</tr>
<tr>
<td>Above 40 years</td>
<td>13</td>
<td>20.3</td>
<td>20.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

Similarly, from Table 4.46 you find that 79.7% of respondents were aged between 18 and 40 years whereas 20.3% were aged above 40 years. Again this was expected as most of the key players in the IT industry in Tanzania were young people aged below 40. This to certain extent might be the effects of the nearly 20-year ICT dormant era in the country discussed in Chapter 1.

4.7 Reflections from the Questionnaires Results

Reflections or rather conclusions drawn from the questionnaires results can be sub grouped into six closely related categories. These include problems related to lack of management support, inadequate planning, inadequate communications, lack of security training, and lack of motivation for security. Let us briefly discuss each of these challenges.
1. *Lack of management support* – Lack of management commitment or support was observed as a major obstacle to security initiatives in many organisations. This was supported by responses in Table 4.29 where only 40% of respondents said their managements were supporting security initiatives. Interestingly in our Seminar 3 which was dedicated to senior executives, participants indicated their serious concerns over security threats and vulnerabilities. Despite the observed senior managements concerns with rise in threats and attacks to computer systems, our research shows that they were slow to respond with financial support. It was learnt that most managements want security quantified on monetary terms. Specifically they wanted to see the projected Return on Investment (ROI) before they commit funds to security projects Casmir and Yngström (2005).

2. *Inadequate communications* – It was also noted that most IT managers and Systems Administrators were not equipped enough to convince their managements to invest in security. Many of them had no security background in concrete terms. Their security knowledge was limited to the technical features that were inherent in a given technical mechanisms. They lacked though the holistic view of security Yngström (1996). This has made it difficult for them to effectively communicate with their managements in order to solicit the management support. In most cases management would like to hear the business language or anything that is related to increased productivity Alberts and Dorofee (2003). Additionally, from Table 4.18 only 15.6% of respondents said their security policies were communicated to all employees. Lack of
effective communications, was therefore, an obstacle to promotion of security awareness.

3. Lack of security training – Lack of specialised security training was observed as another barrier to security initiatives. Both IT professionals as well as other end users of IT systems were lacking appropriate security knowledge. This is partly because there were neither academic institutions nor vocational training centres offering courses on information security per se. From Table 4.20 only 17.2% of respondents had their organisations with formal security awareness programs. However, in Table 4.21 only 6 respondents said their awareness program was targeting all employees. Looking at Table 4.30 you find that only 31.3% of respondents’ organisations conducted at least informal security awareness programs. Considering the economic situation of Tanzania it was unaffordable for most organisations to send their staff abroad for training in security. For example, a 3-day OCTAVE$^2$ Training Workshop offered by CERT/CC was costing $3150.00 for international participants OCTAVE (2005) apart from the transport, accommodation and meals costs. In this case having in-house security training may be a better alternative for most organisations. According to Alberts and Dorofee (2003) OCTAVE typically focuses on organizational risk and strategic, practice-related issues, balancing operational risk, security practices, and technology.

---

$^2$ OCTAVE is an acronym for Operationally Critical Threat, Asset, and Vulnerability Evaluation. It is a risk-based strategic assessment and planning technique for security.
4. *Inadequate planning* – It was learnt that information security was not made part of critical issues during corporate planning. Besides the fact from Table 4.27 that only 39% of respondents had their organisations setting aside a special budget for security of its information assets; in Table 4.28 nearly half of those had that budgets including promotion of security awareness. Likewise in Table 4.17 only 25% of respondents had their organisations with written information security policies. It is natural that organisations do their operations based on documented corporate policies. This means that anything that is not part of the organisation’s policies (such as security in this case) receives negligible attention, if not no attention at all. In fact in many cases security was considered as the IT manager’s or Systems Administrator’s duty. In most organisations there were no budgets for security, especially, for security awareness. This is obviously because security awareness was not a priority during the planning.

5. *Lack of motivation for security* – Since security was not a priority from the planning phase it is explicit that even motivation for it was lacking. Nearly in all organisations studied there was no specific person whose Terms of References (TOR) included supervision and promotion of security awareness initiatives. This was of course expected since the initiatives themselves were not there. Consequently, better performance in security issues were not part of the staff appraisal criteria.

6. *The need for security training at workplaces* – Like in previous chapter, the need for having security training at workplaces was also stressed
from the survey. As may be noted from Table 4.34, 84.4% of respondents acknowledged that information security was a challenge that needed to be addressed in organisations. Expanding on that nearly all (93.8%) of respondents suggested security awareness training to be introduced at workplaces, Table 4.37. In addition, in Table 4.38 about 93.8% of respondents said the awareness program should target all employees.

Findings from this survey tally very well with other finding in phases 1 and 2 as discussed in Chapter 3. Having observed these challenges and based on our personal experience in the field we have proposed an approach that, in our view, would help to raise security awareness in organisations in a cost effective way. We have named it as a ‘Dynamic and Adaptive Information Security Awareness (DAISA)’ approach. The approach is fully discussed in Chapter 6. The DAISA approach takes into consideration the above mentioned six challenges and other key findings discussed in previous Chapters. The approach proposes how to deal with such challenges with a view of raising security awareness.

4.7.1 Deloitte 2005 Global Security Survey

In their 2005 Global Security Survey within the global financial services industry Deloitte³ (2005) came out with some key findings worth to note. They carried out an information security survey in 26 countries in Europe,
Middle East, Africa, Asia and America. In Africa they only surveyed in the North. The said findings were as follows Deloitte (2005, pp. 9-17):

1. Managing compliance now relies on input from multiple stakeholders including technology and security.
2. Organisations need to be prepared for the changing nature of threats such as tsunami in December of 2004.
3. While the number of overall security breaches is down, geography and stature of the organization play a key role in whether an organisation’s security will be breached.
4. There is a trend towards having the Chief Information Security Officer (CISO) report to the highest levels within the organisation.
5. The board’s interest in security is no longer optional; it is a requirement.
6. The most effective way to cost justify the security function is to assess the value and impact delivered to the business.
7. Identity and vulnerability management: The role of these solutions in the compliance world is increasing.
8. Training and awareness are crucial – yet underutilised – contributors to employee vigilance surrounding an organisation’s security function.

On Deloitte (2005, page 17) the report specifically put it that:

“Human performance is a function of ability, motivation and environment. Only 65% of organisations have trained their employees on how to identify and report suspicious activity. Many (64%) were slowly increasing security training and awareness programs, with methods ranging from classroom settings (32%) to posters (20%) to information on web sites (42%) to Lunch &
Learns (18%). Regardless, these programs are only effective if people feel motivated by the overall security objective”.

Key findings in the Deloitte report have many similarities with our DAISA approach proposed in Chapter 6 than there are differences. Table 4.47 attempts to correlate some of the key findings from Deloitte (2005) global security survey report with the key findings, and eventually, key elements of the DAISA approach.

<table>
<thead>
<tr>
<th>Deloitte</th>
<th>DAISA Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Finding #2</td>
<td>Appropriate planning, Dynamic</td>
</tr>
<tr>
<td>Key Finding #4</td>
<td>Management Support, Effective</td>
</tr>
<tr>
<td></td>
<td>Communication</td>
</tr>
<tr>
<td>Key Finding #5</td>
<td>Management Support</td>
</tr>
<tr>
<td>Key Finding #6</td>
<td>Effective Communication</td>
</tr>
<tr>
<td>Key Finding #8</td>
<td>Security Motivation</td>
</tr>
</tbody>
</table>

Possibly, if this survey were extended to Tanzania many of the findings between the two surveys would have been closely correlated. Although Deloitte was targeting financial services industry many of its key findings applies to nearly all business across the board. Indeed even in developing countries there are quite a number of financial services firms that might benefit from the Deloitte findings and recommendations.
4.8 Chapter Summary

In this chapter we have presented the questionnaire design and management. The management of the questionnaires includes distribution, collection and analysis of the questionnaires. Furthermore, we have summarised the reflections from the analysis and interpretation of the questionnaires results. Finally, we have highlighted the key findings from Deloitte (2005) global security survey report in relation to the key elements of the proposed DAISA approach in Chapter 6.
Chapter 5

RELATED PUBLICATIONS

At least five refereed papers were published as part of this research. Four of them were published in different international conferences whereas the fifth paper was published in the Journal of information warfare. In addition, at least five other articles were published in relation to this work. Thus, this chapter presents summaries of the papers and articles that have been published in the course of this research.

5.1 Summaries of Refereed Papers

*Paper 1: IT Security Readiness in Developing Countries: Tanzania Case Study.*

**Summary:**
This paper was presented at the third world conference on information security education Casmir and Yngström (2003a) in Monterey, California, USA. The paper first presents and describes the stepwise development process of Information and Communication Technologies (ICT) in Tanzania citing some examples of major achievements made at that time. It discusses the background of the developments in terms of Television (TV) broadcasting,
establishment of the Internet, Mobile phones, and introduction and use of Automatic Teller Machines (ATM) bank services. The paper gives some statistics on these developments. Furthermore, it discusses the then ‘current situation’ (which is now history) highlighting statistical data of the number of active Internet Service Providers (ISPs) in the country; the number of active Television (TV) stations; number of banks offering ATM services; and describes the progress of the computerization process both in public and private sectors. Also, the paper describes the issues of interconnectivity within and outside the country, citing some ongoing interconnection projects and other related initiatives.

Additionally, the paper gives evaluation results of the security seminars and short courses conducted in Tanzania in year 2001, highlighting the key results of both events. Moreover, it gives in summary some of the major security breach incidents that had been reported and known to the public. The paper concludes by outlining the expected path to addressing information security education issues in Tanzania.

**Paper 2: Security Dimension of IT in Developing Countries: Risks and Challenges.**

**Summary:**
A paper on security dimension of IT in developing countries Casmir and Yngström (2003c) was published in the international Journal of Information Warfare Volume 2, Issue 3. Essentially, the paper discusses security aspects of Information and Communication Technologies (ICT) from the developing countries’ perspective. It starts by highlighting the digital divide issues followed by a discussion on the extent to which computer and computer systems are being deployed and used in Tanzania. The paper describes the proliferation of Internet cafes in Tanzania in comparison to other Southern African Development Countries (SADC). It, also, gives some pricing indication of charges in the Internet cafes and the cross sectional profile of the major customers in the cafes. The paper, further, outlines the main types of services offered at the Internet cafes.

In addition, the paper discusses the pervasiveness of the World Wide Web (WWW) in the country with respect to private business organisations and government agencies. It also, highlights on the extent of the use of Peer-to-Peer (P2P) file sharing technology. The paper further, discusses the issues of licensing in regard to interconnectivity in Tanzania. It gives some statistics on the number of mobile phone subscribers for various mobile phone operators in the country. Likewise, it gives statistical data on the number of Internet subscribers via Dial-Up connections and the corresponding range of monthly subscription fees.
Moreover, the paper discusses issues pertaining to security awareness including responses on how IT security was perceived by many people in Tanzania. It also, discusses the country’s policies in relation to Information and Communication Technologies (ICT). The paper, then presents the observed information security risks and challenges in the country. Specifically, it discusses risks to kids and teenagers when surfing on the Internet. Other challenges discussed in the paper include problems with virus and other malicious codes; password usage; social engineering tricks; and problems related to backup of data in organisations. Security risks facing users, especially teenagers, when using the famous Peer-to-Peer (P2P) software applications across the Internet were also highlighted in this paper. The paper concludes by suggesting some remedial course of actions to be taken.

A full paper can be obtained in the international Journal of Information Warfare Volume 2, Issue 3, from page 38-47; ISSN 1445-3312.
**Paper 3: Information Security Education for Developing Countries: The Challenges.**

**Summary:**
This paper on information security education for developing countries Casmir and Yngström (2003b) was presented at the second summer school workshop on Risks and Challenges of the Network Society, organised by IFIP WG 9.2, 9.6/11.7, 9.8; Karlstad, Sweden. The paper commences by highlighting on the bold steps that have been taken by the government of Tanzania in recognising the importance and the power of Information and Communication Technologies (ICT). The steps discussed in the paper include development of the national ICT Policy as part of the implementation of the country’s development vision 2025. Furthermore, it discusses the domestic digital divide or simply rural-urban digital divide in the country.

In addition, the paper discusses the difficulty in grasping IT security concept linking it to the delayed embarking of the country to world of information and communication technologies. It then, discusses the country’s cultural and ethical aspects in relation to IT security. Scarcity of, and higher demand for competent IT professionals in Tanzania was also highlighted in the paper. Similarly, issues pertaining to scarcity of and higher demand for competent information security specialists in the country have been discussed in the paper. The paper also discusses the observed low level of security awareness to many people in Tanzania.
Additionally, the paper goes on suggesting that one of the ways to improve security awareness in the country is to apply an ‘anvil and hammer’ approach meaning that there should be academic level security education in line with awareness programs at workplaces. The suggestion was based on the observed fact that there were a large number of practitioners in the country using computer systems without having proper training on security basics. Specifically, the paper states that it was rather not practicable to take them all back to formal classroom education on security issues. The paper concludes by suggesting that sort of vocational training centres focusing on information security training and awareness should be established in the country to address the problem at hand.

A full paper is available in the proceedings of the Second Workshop on Risks and Challenges of the Network Society, by IFIP WG 9.2, 9.6/11.7, 9.8; Karlstad, Sweden.

Summary:
Another paper is on intrinsic legal issues in IT security Casmir and Yngström (2004) which was presented at the fourth conference on information security in Johannesburg, South Africa. The paper begins by outlining the great global market opportunities to both consumers and entrepreneurs that are created by the advancement in the Internet-based procurement or more precisely e-commerce. Specifically, the paper discusses issues pertaining to e-invoicing, e-contracting, e-government, e-auction and e-reverse auction, just a few to mention. It attributes higher speeds for information propagation over the World Wide Web (WWW) and wider outreach of the market segment as key advantages of e-commerce. The paper, however, cautions that despite all these enormous benefits of e-commerce there were increasing concerns on governance and control of information traversing over the Internet around the globe.

In particular, the paper discusses aspects of informational privacy in the cyber world making references to a number of Privacy Acts as applied in different jurisdictions. Nonetheless, the paper cites lack of interoperability of Privacy Acts of different jurisdiction as a vulnerability that might be exploited by the cyber criminals to cause harm. The paper also discusses various issues pertaining to Copyrights and other Intellectual Property Rights (IPR) over the Internet. Additionally, the paper highlights on various fraudulent activities over the net citing some examples of such incidents that have been discovered in different countries. It further, discusses what makes it easier for fraudsters
to succeed in their missions. Furthermore, the paper discusses electronic signature vis-à-vis digital signature, citing differences in the interpretations of the two in different jurisdictions as an issue to be resolved. The paper cites human as the focal point of legal-IT related problems in the cyber world.

On concluding the paper suggests three different approaches to address the legal-IT related problems. The suggested approaches include establishment of interdisciplinary academic curricula in which Law students shall get opportunities to learn on what IT systems are, how they work/operate, and their capabilities and limitations. Likewise, the students doing IT-related academic programs get opportunities to learn about the law, what it does and what it does not do. The idea behind this suggestion, the paper states, was neither trying to convert IT specialists into lawyers nor lawyers into IT professionals but rather to make the two ‘talk the same language’ when it comes to legal-IT related security issues in e-commerce. Another suggestion was interweaving computer ethics topics into primary and secondary level education. The third suggestion was to synchronise e-commerce related laws globally.


Summary:
This paper titled towards a dynamic and adaptive information security awareness approach Casmir and Yngström (2005) was presented at the fourth world conference on information security Education in Moscow, Russia. Essentially, the paper presents and discusses the initial findings of this research. The paper commences by describing the pace of computerisation processes in Tanzania as of the end of year 2004 in comparison with three years before. It then highlights on various research activities that has been going on from 2001 to 2004 with respect to raising information security awareness. It gives some statistics of the number of people that have been trained in security awareness as part of this research. The paper describes the creation of multidisciplinary integrated security awareness, training and education approach as the most effective way of addressing security awareness issues in Tanzania.

Of particular interest, the paper presents and discusses some key results that have been revealed as adversely affecting the promotion of effective security awareness in the country. Of these, cultural aspects were cited as being among the hindrances. The paper gives a couple of statistical data from the respondents on how they perceived information security. As much as 65% of the respondents were not even aware of what information security was all about whereas about 58% of the respondents perceived information security as a ‘new culture’ attributing it to IT staff only. Lack of management support to
security was another key finding cited in the paper. The paper also mentions budgetary constraints as another key finding of the barriers to security awareness initiatives in organisations. The paper further, mentions lack of country-level information security policies and guidelines as one of hindrances to security awareness initiatives. Lack of motivation to employees in relation to their participation or involvement in security related matters was another barrier to effective security awareness mentioned in the paper.

In conclusion, the paper presents and describes the evaluation and impacts of various research activities that has been going on in the past three or more years. The paper also highlights on the prospective Dynamic and Adaptive Information Security Awareness (DAISA) approach to address security awareness issues not only in Tanzania but also elsewhere.

A full paper is available in the proceedings of the Fourth World Conference on Information Security Education (WISE-4), organized by IFIP Working Group 11.8 (IT Security Education), Moscow, Russia; ISBN 5-7262-0565-0.
**Paper 6: Security Dimension of E-Government:** Trust and Confidence.

**Summary:**
This paper on security dimension of e-government with emphasis on ‘Trust and Confidence’ Casmir (2004d) was presented at the East African Regional E-Government Workshop in November 2004. The workshop hosted by the Government of Tanzania was held at the Dar es Salaam International Conference Centre (DICC) in Dar es Salaam, Tanzania. The paper begins by highlighting on the increased society’s dependency on computer-based technology in the region as well as worldwide. It then attempts to define e-government as “Government’s use of information and communication technology, particularly web-based Internet applications, to enhance the access to and delivery of government information and services to citizens, employees, suppliers, business partners, and other government agencies”. Adding that specifically, e-government refers to the use by government agencies of information and communication technologies say, the Internet, LAN/WAN and other computing infrastructure that are capable of transforming relations with citizens, businesses and other government agencies. In addition, the paper outlines the typical activities of e-government, benefits and drawbacks of e-government. It also, outlines the seven rules for e-government based on Kalakota and Robinson (1999).

Additionally, the paper discusses challenges that are facing e-government implementation including information security, privacy issues, and public policy issues just a few to mention. The paper then, discusses issues pertaining to building confidence and trust in e-government among potential
stakeholders. Particularly, the paper singles out ‘Trust and Confidence’ among participating parties in the e-government process as of paramount importance for the effectiveness and success of any e-government initiative.

5.2 Summaries of Newsletter Articles

Newsletter articles were also published as part of this work. All the five articles on different security topics have been published in the University of Dar es Salaam Computing Centre (UCC) Newsletter which is published on quarterly basis. The newsletter is quite popular in Tanzania and is read by a wider and heterogeneous audience. A series of these Newsletter articles is primarily aiming at raising security awareness to the majority at relatively lower cost. Production of the Newsletters is fully funded by the University of Dar es Salaam Computing Centre (UCC), and they are freely distributed to various organisations and individuals. This section, thus, summarises the articles.

**Article 1: Information Security: The Concept.**

**Summary:**

Article one on information security concept was published in UCC Newsletter Volume 1 Issue 1 Casmir (2004a). The article was primarily aiming at highlighting the readers on what information security is all about. It begins by defining today’s era as an information age which is typically characterised by extensive use of computers and computer systems, specifically, in a networked environment. It then compares traditional manual means for information handling vis-à-vis electronic means. The article then describes the traditional computer security whereby the emphasis was more on protection of physical computers than data and information inside the computers. It further, discusses the complexity of handling information in a networked environment,
especially, over the Internet. The article then, describes what information assets are; who may compromise these assets; and for what motives. The article ends by highlighting on the importance of protecting the information assets and discusses various security counter measures.

A full version of the article is available in the UCC Newsletter Volume 1 Issue 1, Page 5 and 9, April-June, 2004; ISSN 0856-9673.

**Article 2: Understanding a Computer Virus and Antivirus Protection Strategy.**

**Summary:**

This article on computer virus and antivirus protection strategy has been published in UCC Newsletter Volume 1 Issue 2 Casmir (2004b). The article commences by recalling on Melissa virus in March 1999 and the ILOVEYOU virus in May 2000 as some of the deadly computer virus that were still in memories of many. It then, defines a computer virus and its typical characteristics namely replication, concealment and bomb. The article also, compares a computer virus vis-à-vis a biological virus by highlighting their similarities and differences. It also, mentions file extensions that are commonly assumed by computer viruses such as .pif, .exe, .scr, .vbs and files with double extensions such as .doc.pif.

In addition, the article defines other malicious codes such as Worm, Macros and Trojan horse distinguishing them from a typical computer virus. It then, describes different types of computer viruses. The article further, describes
how a virus gets into a computer and how it executes. Moreover, the article outlines various virus protection strategies including a layered approach to virus protection. With a layered approach, the article describes the desktop or workstation virus protection followed by email server protection and finally network gateway protection. The article concludes by highlighting on user awareness for virus threats including some useful hints for virus protection.

A full version of the article can be read in the UCC Newsletter Volume 1 Issue 2, Page 2-3, July-September, 2004; ISSN 0856-9673.

**Article 3: Understanding a Firewall and How it Works.**

**Summary:**

Article 3 on understanding a firewall and how it works was published in the UCC Newsletter Volume 1 Issue 3 Casmir (2004c). Essentially, the article was meant to educate computer and network users on the capability and limitations of the firewall. It begins by defining what a firewall is and how it works in principles. The article then, describes the various types of firewalls including hardware firewalls and software firewalls. It also, highlights their similarities and differences. In particular, the article describes network layer firewalls and application layer firewalls. It then, outlines their advantages and disadvantages. Additionally, the article describes the De-Militarized Zone (DMZ), its functions and its importance in the network infrastructure. The article ends by advising the readers to use firewalls for enhanced security of their networks.

A full version of the Newsletter is available in the UCC Newsletter Volume 1 Issue 3, Page 1-2, October-December 2004; ISSN 0856-9673.
**Article 4: About Virtual Private Network (VPN).**

**Summary:**
This article on Virtual Private Network (VPN) has been published in the UCC Newsletter Volume 2 Issue 1 Casmir (2005a). The article was, specifically, targeting organisations that have their businesses spread across the country as well as outside the country. As discussed in Chapter 1 many private and public business organisations have interconnected their sub offices in different regions in the country and others are in the process to do so. The article, therefore, commences by describing on what constitutes a Virtual Private Network (VPN) followed by outlining its many advantages. It then, describes the different types of VPN implementations including their similarities and differences in terms of technical functionalities. In addition, the article highlights on the costing aspects of the VPN implementations vis-à-vis security and reliability. The article concludes by urging organisations with interregional and international presence to consider implementing VPN to protect their data and information traversing over the net.

A full version of this article is available in the UCC Newsletter Volume 2 Issue 1, Page 2-3, January-March, 2005; ISSN 0856-9673.
**Article 5: Performing IT Risk Analysis.**

**Summary:**
Article five on performing IT risk analysis has been published in the UCC Newsletter Volume 2 Issue 2 Casmir (2005b). Essentially, the article was aiming at highlighting the readers on the basic steps in performing IT risks analysis in their respective organisations. The article commences with the assertion that for an organisation to succeed in the implementation and use of IT systems it needs first to study, understand, identify, and properly administer the many risks and threats emanating from the use of IT systems. It then, describes what IT risk analysis is all about.

In addition, the article outlines some of the major reasons for performing IT risk analysis in an organisation. Some of the reasons mentioned in this article include to:

- Improve security awareness amongst staff
- Identify IT assets, vulnerabilities and appropriate security controls
- Improve basis for decision making, especially, when it comes to budgeting for security
- Justify expenditures for security measures

Moreover, the article outlines six basic steps to follow when performing an IT risk analysis. Such steps include 1) identify IT assets; 2) determine security vulnerabilities; 3) estimate likelihood of exploitation of the identified vulnerabilities; 4) compute expected annual loss; 5) survey applicable security controls and their respective costs; and 6) Project annual savings of the
controls. The article ends by advising the readers to involve a specialised information security specialist when performing risk analysis for their organisations.

A full version of the article is available in the UCC Newsletter Volume 2 Issue 2, Page 2, April-June, 2005; ISSN 0856-9673.

5.3 Reflections from the Papers and Newsletter Articles

Both the papers and newsletter articles were not only informative but also educative. A wider audience have had opportunities to read these publications and, we believe, have learned something in due course. Moreover, this is not the end of writing such publications but rather the beginning of it. We plan to prepare many more of such publications as it may deem necessary. In addition, comments and suggestions from part of the audience that have read the papers and other articles have contributed significantly to the improvement of the proposed DAISA approach.

5.4 Chapter Summary

In this chapter we have presented summaries of publications that have been written as part of this work. We started by presenting summaries of refereed papers followed by summaries of Newsletter articles. All of these publications were written with a view of raising security awareness not only in Tanzania but also elsewhere. The chapter has been concluded by highlighting some of the reflections from the papers and newsletter articles.
Chapter 6

THE DYNAMIC AND ADAPTIVE INFORMATION SECURITY AWARENESS (DAISA) APPROACH

This chapter presents and describes the Dynamic and Adaptive Information Security Awareness (DAISA) Approach. The chapter begins by defining the approach and its purpose followed by the key elements of the approach. Then it gives detailed descriptions of the functions for each of the key elements and how they interrelate. It also, outlines the strategies for implementing the approach. The chapter concludes by discussing the validation aspects of the DAISA approach using action research methodology.

6.1 Overview of the DAISA Approach

To accomplish this research there have been a number of related activities. As highlighted in Chapter 1 the main activities include seminars and short courses on IT security; interviews; focus group; security survey using questionnaires; and writing publications. Security awareness was cited in all of these events as ‘the fundamental element’ in protecting information assets (see Chapter 3). This fact predisposed us to develop an effective approach to address information security awareness. Following discussions in previous chapters it is clear that in Tanzania, and possibly in many other countries, the weakest link in a security chain is people. Pfleeger (1997); Schneier (2000) and
Mitnick and Simon (2002) all refer to human as the weakest link in a security chain. Mitnick and Simon (2002, pp.4) specifically say that as security technologies improve and systems become more difficult to exploit “attackers will turn more and more to exploiting the human element”. Exploitation of the human element manifests itself in many different ways including social engineering tricks. Alas, from Table 4.43 in Chapter 4 only 25% of the respondents were at least aware of social engineering tricks. Such results were not good signs given that social engineering tricks are so prevalent nowadays.

It is against this background that we propose the DAISA approach for security awareness. The approach is meant to address the human element of information security rather than the technology aspects. The DAISA approach contains two keywords namely Dynamic and Adaptive. Based on our methodology and on the general system theory, a typical IT system in a real-world is an active system which is complex; adaptive; self-regulating; and open to the environment (see Chapter 2). To effectively deal with such a system you need to apply measures that are dynamic and adaptive in nature. The DAISA approach is technically designed to help organisations in developing countries in creating and maintaining effective security awareness. Perhaps let us first define the two keywords of the DAISA approach ‘Dynamic’ and ‘Adaptive’. This is because same words can mean different things in different contexts.

……..Dynamic
By the term Dynamic in this context we simply mean that the approach is flexible to change with Information Technology advancements. The
dynamicity of the approach also means to be flexible with the ever changing cyber threats and vulnerabilities to information assets. Dynamic in this case also means that the DAISA approach is flexible towards varying organisational cultures.

Adaptive
Adaptive in this context means that it should be easier to integrate the approach into organisations’ business processes without disrupting them. Adaptive here also means that the DAISA approach is agile and responsive to the specific security requirements of the organisation in question. It also means that organisations themselves as systems need to be adaptive in their practices to give a room for building security awareness culture. The approach is adaptive in the sense that it is capable to rapidly respond to changes in business environments and changing security threats.

Combining the descriptions of the two keywords (i.e. Dynamic and Adaptive) one can easily understand what the DAISA approach is. By definition, it is the approach that is meant to stepwise guide organisations to build security awareness cultures in developing countries. The approach that will act as a change agent towards security awareness in developing countries; and that will provide generic guidelines to achieve effective security awareness. The approach aims at both administering and controlling security as well as coordinating and promoting security awareness in organisations.
6.2 Key Elements of the DAISA Approach

Having defined the DAISA approach let us now take a look at the key elements of the approach. There might be numerous factors that can make security awareness a success depending on the context. However, the DAISA approach employs six of those. The 6-key elements of the DAISA approach have emerged out of the findings from the research as illustrated in Chapters 3, 4 and 5. The 6-key elements include:

1) Management Support  
2) Effective Communication  
3) Security Motivation  
4) Appropriate Planning  
5) Relevant Training Material  
6) Continuity and Consistency

In the following section we are going to describe each of the six key elements and its functions in the DAISA approach. The order in which the key elements appear in the list does not matter that much, what counts most is the significance and function of each of these key elements in the effectiveness of the DAISA approach. If we are to put them in order of priorities then management support together with appropriate planning would come first, and the rest would follow. This is simply because other key elements are very much dependent of these two.
1) Management Support

Management support is fundamental and critical to the success of any security awareness program in an organisation. From the questionnaires when asked whether their managements were supporting or committed to information security initiatives 45.3% of the respondents were not sure whereas 14.1% responded with a ‘No’. Only 40.6% responded ‘Yes’. Table 6.1 presents the full results of this query.

<table>
<thead>
<tr>
<th>Response</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>26</td>
<td>40.6</td>
<td>40.6</td>
<td>40.6</td>
</tr>
<tr>
<td>No</td>
<td>9</td>
<td>14.1</td>
<td>14.1</td>
<td>54.7</td>
</tr>
<tr>
<td>Not Sure</td>
<td>29</td>
<td>45.3</td>
<td>45.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>64</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

In any organisation the management is the one that decides, budget, and allocate financial and other resources within the organisation. It is, therefore, critically important to have the full management support on security awareness initiative. Figure 6.1 represent Management support as one of the six building blocks of the DAISA approach. However, for the management to get committed and to fully support security awareness; they first Hall (2001) need to have a better understanding of the criticality of security threats, risks, and vulnerabilities in relation to their organisations’ business objectives.
This can be achieved in either of the two ways. One is that an influential management team member happens to attend an information security awareness seminar somewhere and thoroughly briefs the management on return. This can effectively work but the likelihood of happening is narrow. This is because members of the management are usually very busy with other duties therefore a few can afford to dedicate their time for such a seminar. From our experience gained during this research, when you invite the senior executives to a day-long seminar or more they tend to send their subordinates instead. The second alternative is for someone from within or outside the organisation to plan, build a business case around security awareness and present it to the management for endorsement. This is a more feasible alternative and highly recommended for the DAISA approach. Detailed techniques on how to build a business case for the management are discussed in Section 6.3 ‘Getting started’. The DAISA approach requires that unless the management makes information security awareness a priority it will never be effective.
2) Effective Communication

Effective communication Guenther (2004) is a key to the success of the DAISA approach. For example in item (1) above we described the functions and importance of management support. However, if at all we cannot effectively communicate with the management which is responsible for decision making and resource allocation we run the risk of our proposals’ for security awareness to be turned down. In this case the better we effectively communicate our security awareness proposals to the management, the more likely that the management will respond positively. This makes the second building block of the DAISA approach as shown in Figure 6.2.

![Figure 6.2: Effective Communication Dimension](image)

Effective communication in this context goes beyond communicating to the management. We also need to communicate the security messages to the end users effectively. This means that we need to avoid technical jargons by using simple yet understandable language. The purpose of effective communication to the end users is not only to convey a security message but also to ensure that the message conveyed is properly interpreted to its original meaning and intention. We conclude this item by the assertion that however good the security awareness idea may be if it is not effectively communicated to the
stakeholders it is likely to fail, especially, when it comes to the implementation aspects.

3) **Security Motivation**

It has been learnt that people in Tanzania, and perhaps many other people elsewhere, would like to know ‘what is in it for them’ prior to engaging themselves into a particular activity or task. In other words, there must be some sort of motivations Parker (2002); Parker (1998) to make people fully participate in security awareness activities besides their normal job functions. Without motivation Munley (2004) security awareness effort is unlikely to bare the desired fruits. Security motivation may come in many different forms. Figure 6.3 presents Security Motivation as another building block of the DAISA approach.

![Security Motivation Dimension](image)

**Figure 6.3:** Security Motivation Dimension

One way to ensure security motivation that we recommend in this approach is to link security in way with job performance. It has to be made part of staff appraisal criteria. For example a staff that has timely reported the most critical security incident in the organisation or has dealt with a particular security threat appropriately should be reward during staff appraisal. The reward for
this should be tangible enough to make others emulate from their colleague. Typical rewards may range from monetary terms to promotion, and the like.

4) **Appropriate Planning**

Security Awareness, like many other corporate activities, requires a comprehensive planning. Planning in this context is a visionary process that takes care of fast technological advancements; changes in business requirements of the organisation; ever evolving security threats and vulnerabilities; and varying organisational cultures and practices. Planning also here means a careful integration of security awareness program into the organisation’s business processes without disrupting them. Figure 6.4 shows the Appropriate Planning as another element of the DAISA approach.

![Figure 6.4: Appropriate Planning Dimension](image)

Security awareness cannot be a one-man effort. Everyone has a role to play. It needs a coordinated effort of every individual in the organisation. Planning further means enhancement of the security posture of the organisation. Again planning also includes dedicating a person solely responsible for overseeing the development, management and promotion of a security awareness program in an organisation. It is through planning that an organisation can develop a
comprehensive information security policy to guide the security implementation and awareness processes. Planning also means making security a priority. While we are talking of making security a priority area at an organisational level today; other countries including Australia Armstrong (2003), Sweden Yngström (1996), and United States of America Wilson and Hash (2003) have already made information security a national level priority. When making corporate budget security awareness should be one of the core activities to be budgeted for right from the beginning. A totality of these is what we term as appropriate planning in the DAISA approach.

5) Relevant Training Material

No matter how best you plan if at all the material and other tools that are used to deliver the security awareness message are not relevant to that specific situation it is going to be very difficult to achieve the intended goal. It should be noted that security is not a ‘one-size-fits-all’ feature; it is rather a context dependent process. In this case training materials and other teaching aids should be designed in a way that is tailored to that specific environment. Together with the general security awareness materials, it might be a good idea if some of the training material and examples cited are tailored to the specific job functions. Therefore tailoring training materials; other teaching aids; and relevant examples to specific job functions is such an important element in the DAISA approach as presented in Figure 6.5.
Senior management, for example, would prefer anything that is related to increased productivity, hedging shareholder value, enhanced business continuity and the like. Accountants on the other hand, are most likely motivated with something that is related to financial fraud detection and prevention. Likewise, people in the human resource department would perhaps be more interested in issues pertaining to privacy, legal, ethical, and policy compliance.

6) **Continuity and Consistency**

Security learning continuum is a lifelong learning process. It is not an issue of hiring an information security consultant for some days or even years and then let the consultant go without appropriate measures in place. That is a reason in item (4) above we recommended dedication of a person or a team of people to specifically deal with security issues as their main terms of reference (TOR) at all times as long as an organisation is in existence. In Figure 6.6 we present the sixth dimension of the DAISA approach, which is Continuity and Consistency. It is the nature of human being that we tend to forget things with time, it is therefore, critically important to keep people reminded and updated.
on security awareness matters. The security message should be continuous and consistent in such a way that it permeate through the entire organisation and ultimately become part of the organisational culture.

According to SAI (2005) the use of various reminder tools such as posters and banners carrying security awareness messages in very important in keeping the security message live. Other advantages of using reminder tools include to:

- invoke cultural change
- keep the security message fresh
- continual education (informally), and
- keep security interests alive among employees

To sum up, these are considered as the critical success factors of the DAISA approach. Taken together they form a hexagonal DAISA model as illustrated in Figure 6.7.
If one or more of the six components is missing then the hexagon is incomplete thus the effectiveness of the DAISA approach is relatively at stake.

### 6.3 Getting Started

For great things to happen they need to be initiated. Security awareness process is no exception. Like a Chinese proverb that states ‘A journey of a thousand miles starts with one step’. There could be many different ways to initiate security awareness process in an organisation, but given the situation in Tanzania, and perhaps in many other developing countries, we recommend these two.

1. Hiring a consultant who is specialised in Information security, or
2. Sending one or more of your IT staffs to a specialised training in Information Security
Regardless of which way an organisation opts to go for, the end point is to have someone knowledgeable enough to initiate the move. This person(s) should build a business case around information security awareness and present it to the management for scrutiny and eventually endorsement. The case should commence by performing a comprehensive IT risk analysis and then clearly showing how security awareness can play part to reduce the risk in a cost effective way. We do not give details of risk analysis here as it is beyond the scope of this work. Likewise, we do not give details of the content of training material for security awareness here as this will very much depend on the time, context and objectives of the implementing organisation. However, the use of posters, fliers and other multimedia teaching aids with security awareness messages is highly recommended for effectiveness of the security awareness programs. For the implementation of the DAISA to be effective there are at least ‘four key steps’ to be observed by the implementers from the very beginning.

1) To identify existing coverage of security awareness in an organisation (if any)
2) To identify specific areas of focus for their security awareness programs
3) To specify a baseline of security knowledge required for their employees
4) To measure effectiveness of their security awareness programs based on the pre-defined security awareness metrics (discussed in the succeeding section).

If items (1) to (3) above are systematically accomplished, that will enable the implementer of the DAISA approach to confidently identify ‘the gap’ between
existing level of security awareness and the required level in the organisation. Then the awareness program should specifically aim at covering that gap as illustrated in Figure 6.8.

![Figure 6.8: Security Awareness Knowledge Gap to be addressed by DAISA Approach](image)

To start with the author and at least three other colleagues are available and willing to assist any interested organisations in implementing the DAISA approach.

### 6.4 Security Awareness Metrics

To be able to measure the effectiveness of a security awareness program at a workplace the DAISA approach requires that there should be some sort of predefined ‘security awareness metrics’. In this context, security awareness metrics are sort of quantifiable measurements or any identifiable attributes that collectively characterise changes in security awareness of employees. It is against those metrics the effectiveness of the program can be measured.
Security awareness metrics may vary from one organisation to another depending on business environment of the organisation in question. The typical security awareness metrics might include but not limited to the following:

1. Increased number of reported security incidents
2. Reduced number of helpdesk calls on virus related problems
3. Reduced number of virus or other malicious code outbreak
4. Increased comments on the security awareness program
5. Reduced number of cases for use of pirated software
6. Reduced traffic to unethical websites such as pornographic sites and the like.
7. Decreased number of viruses problems resulting from opening unexpected email attachments
8. Decreased number of malicious codes attacks resulting from downloading contents from untrusted web sites
9. Increased adherence to backup routines and procedures, and many more.

Security awareness metrics should be reviewed on regular basis. During the review new metrics should be developed and those found obsolete should be discarded. Each organisation should develop its own set of security awareness metrics.
6.5 Implementation Strategy for the DAISA Approach

For a security awareness program to be effective it has to be recursive and must be evaluated on regular intervals based on predefined corporate security awareness metrics. Every organisation has its own specific and sometimes unique business objectives. Security awareness implementation should, therefore, be designed in line with the business objective of a given organisation. Likewise the security awareness metrics should base on the corporate business objectives as well as business environments.

An organisation’s information security awareness program should be recursive and cyclic in nature as depicted in Figure 6.9.

![Figure 6.9: An Information Security Awareness Program Life Cycle](image)

During the planning stage an information security policy has to be developed to guide implementations of the program. We recommend the policy to be kept as short as possible yet comprehensive enough to make it enforceable. A
policy that is too long and complicated to comprehend will be difficult to follow. A maximum of 2-page is a recommended length of an enforceable policy. The policy should clearly state what is allowed and what is not. It should also indicate the corresponding penalties in case of misuse or abuse of the information assets. The policy must be well communicated to all staff in the organisation. Staffs should also be given an ample time to discuss it and give their comments on the policy. This will serve two purposes. First, it will make them feel part of that policy (participatory element); and second it will make them to fully understand the policy.

In the course of implementation of the awareness program proper documentation of all security incidents should be done. Nothing should be taken for granted. This means that everything however little it may be should be properly recorded for evaluation purposes and for staff appraisal. We recommend an annual evaluation of the program. A team with representation from all functional departments in the organisation should be formed to carryout the evaluation of the program. Taking on board recommendations from the evaluation team the plan should be amended accordingly and reimplementation should start once again. The process should continue in that fashion for as long as the organisation is in existence. By working together people in an organisation shall be able to understand the risks associated with the use of IT systems and be in a position to protect the organisation’s information assets. Table 6.2 shows tasks vis-à-vis the responsible parties.
Table 6.2: Tasks and Responsible Parties

<table>
<thead>
<tr>
<th>Phase/Task</th>
<th>Responsible</th>
<th>Key Element</th>
</tr>
</thead>
</table>
| Plan/Initiate     | • Management Team  
• Security Awareness Team  
• Representatives from all Functional Departments  
• External Consultant | All         |
| Implementation    | • All staff under guidance of the security awareness team                    | All         |
| Evaluation        | • Management Team  
• Security Awareness Team  
• Representatives from all Functional Departments  
• External Consultant (if possible) | All         |
| Amendment of the Plan | • Selected members from the evaluation team                                   | All         |

From Table 6.2 it can be noted that all the six key elements of the DAISA approach should be observed at every step of the security awareness life cycle. A composition of the security awareness team should include at least one of the management team members. This is critically important to ensure that the management is fully informed of all activities of the security awareness program at all times.

6.5.1 Training Adults

It is most likely that a segment of people to be trained in organisations are grown-ups or simply adults. This concern was also cited by the members of the critique group in Chapter 3. Training adults in something relatively new like security awareness might somewhat be tricky and challenging. Most of those may not be very much conversant with computers and the Internet.
facility. In such cases you need to devise better ways of making them learn and find it fun for them. A fun way to let adults comprehend something new is using experiential learning concepts. Thus, adults may learn better when you build a new concept around something they are familiar with. This way, security awareness can be made fun for them and thus be more effective.

6.6 Keeping Pace with Changing Cyber Threats and Vulnerabilities

Information technology is changing very fast so does cyber threats and vulnerabilities. To keep pace with ever evolving security threats and vulnerabilities, the DAISA approach requires that those in charge of security awareness in organisation should get updated regularly. We recommend that at least once a year one or more from the security awareness team should attend a high level information security conference or workshop. This will help to keep the in charge well informed on emerging new threats and vulnerabilities and consequently learn new ways of dealing with them. It is expected that on return they will disseminate the knowledge gained to the rest of the organisation. For this to work though there should be a budget set aside for it right from the beginning.

6.7 Security Awareness as Part of Organisational Culture

For security awareness to be effective it should fully permeate into the entire organisation. In other words it should form part of the organisational culture. Robins (2003, pp 231) defines organisational culture as
“...a system of shared meaning held by members that distinguishes the organisation from other organisations. This system of shared meaning is, on closer examination, a set of key characteristics that the organisation values.”

Robins (2003) further describes the five functions of organisational culture that:
1) It has a boundary-defining role; that is, it creates distinctions between one organisation and others.
2) It conveys a sense of identity for organisation members
3) It facilitates the generation of commitment to something larger than one’s individual self-interest
4) It enhances social system stability
5) It serves as a sense-making and control mechanisms that guides and shapes the attitudes and behaviour of employees.

This last function is of particular interest to us. If security awareness message is effectively communicated to all staff; and if security initiative has full support and blessings of the management it is likely that security awareness will be adopted by all staff. For security awareness to become part of the organisational culture it has to be initiated, implemented and maintained as described in Section 6.5 above.
6.8 Validation of the DAISA Approach

Perhaps we need to hold on and recall our methodology before getting deeper into the validations of the DAISA approach. As stated in Chapter 1 our methodology is action research. The reasons for choosing this methodology have been discussed at length in Chapter 1. Nonetheless, this section shall reiterate part of what has been discussed in Chapter 1 with a view of clarifying the validation of the DAISA approach.

There are numerous definitions for action research all of which are dependent on the definers’ contexts. For example, Kemmis and McTaggart (1990, pp.5) defines action research as a “form of collective self-reflective inquiry undertaken by participants in social situations in order to improve the rationality and justice of their own social or educational practices, as well as their understanding of these practices and the situations in which these practices are carried out”.

According to McCutcheon and Jung (1990, pp.148) action research is defined as a “systemic inquiry that is collective, collaborative, self-reflective, critical and undertaken by participants in the inquiry”.

In another definition by Rapoport (1970, pp. 499) as cited in McKernan (1991, pp. 4) says “action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework”.

174
A close examination of the three definitions for action research according to Masters (1995, pp. 3) reveals four common themes namely empowerment of participants, collaboration through participation, acquisition of knowledge, and social change. These are the very key elements a properly done action research has to incorporate; and against which its validity is assessed. According to McNiff (2002, pp. 22) validation of action research is done through a critique group. Members forming the critique group should be part of the stakeholders of the society in question. This was done in Chapter 3 using a group of 40 practitioners as a critique group. In fact the idea about development of the DAISA approach emanated from that critique group as discussed in the evaluations in Chapter 3.

In addition, Grundy and Kemmis (1981) as cited in Grundy (1988, pp. 353) state three conditional requirements for the validity of an action research. These are as follows:

1) The research takes as its subject matter a social practice, regarding it as a strategic action susceptible to improvement.
2) The research proceeds through a spiral of cycles of planning, acting, observing and reflecting, with each of these activities being systematically and self-critically implemented and interrelated.
3) The research involves those responsible for the practice in each of the moments of the activity, widening participation in the project gradually to include others affected by the practice and maintaining collaborative

Furthermore, Grundy and Kemmis (1981) state that the three conditions are the necessary and jointly sufficient conditions for the validity of the action research. Based on these three conditions, the development of the DAISA approach suitably complies with them all as illustrated hereunder. The fact that a field work for this research was conducted in a developing country, Tanzania, including seminars, short courses and questionnaires survey illustrates compliance to condition number one. Likewise, since our research went through 2 phases in a cyclic (i.e. planning, acting, observing and reflecting on each cycle) manner, then this illustrates compliance with condition number two above. Condition number three was met through involvement of the stakeholders at all stages of the research from the planning to execution, to evaluation phase as detailed in Chapter 3.

Additionally, like for the case of the definitions of action research, there are different types of action research. For example, McKernan (1991, pp.16-27) describes three types of action research as follows:

a) Type1 – The scientific-technical view of problem solving.

b) Type2 – Practical-deliberative action research.

c) Type3 – Critical-emancipatory action research.

In other developments Grundy (1988, pp. 353) describes what is referred to as ‘modes’ of action research. Grundy describes the three modes of action
research as “technical, practical, and emancipatory”. Furthermore, Holter and Schwartz-Barcott (1993, pp. 301) describes three types of action research as comprising of “a technical collaborative approach, a mutual collaborative approach and an enhancement approach”. Also, McCutcheon and Jurg (1990, pp. 145-147) describe what they call three perspectives of action research as “a positivist perspective, an interpretivist perspective and a critical science perspective”.

Combining key concepts from different descriptions of perspectives of action research as discussed above, Masters (1995, pp. 3-8) formulates and discusses three generalised types of action research as follows below.

Type 1: Technical/Technical-Collaborative/Scientific-Technical/Positivist

Masters (1995) describes the primary objective of the researcher in this approach as to investigate and test a specific intervention based on a pre-specified theoretical framework; adding that “the nature of the collaboration between the researcher and the practitioner is technical and facilitatory” Masters (1995, pp.3). In this case, the researcher identifies the problem and a particular intervention thereafter practitioners are involved and they agree to facilitate with the implementations of the intervention Holter and Schwartz-Barcott (1993, pp. 301). According to (Grundy 1982, pp. 360) communications in this type of research are mainly between the facilitator and the group to ensure effective communication of the ideas to the group.
Type 2: Mutual-Collaborative/Practical-Deliberative-Interpretivist Perspective

Type 2 of action research according to Masters (1995) is mutual-collaborative in nature. Both the researcher and practitioners jointly discuss and define the problem to be investigated by mutual consensus. Flow of communications in type of action research according to (Grundy 1982, pp. 360) should “be unimpaired between each member of the group and the facilitator”.

Type 3: Enhancement approach/Critical-Emancipatory Action research/Critical Science perspective

Masters (1995) discusses type 3 of action research as Enhancement approach or Critical-Emancipatory action research. Emancipatory action research according to Masters (1995, pp. 6) “promotes emancipatory praxis in the participating practitioners; that is, it promotes a critical consciousness” that manifests itself in practical action to promote change. In this type of action research there should be symmetrical communication flow between the facilitator and practitioners from which enlightenment flows (Grundy 1982, pp. 360). Table 1.1 in Chapter 1 summarises the detailed descriptions of the generalised three types of action research according to Masters (1995). Discussions made in this section briefly specify criteria used in validating the DAISA approach based on action research methodology.
6.9 Chapter Summary

In this Chapter we have presented and described the DAISA approach. The approach has been developed with a view of raising information security awareness in developing countries. We have defined the six key elements of the approach and how they relate to each other. Then we have highlighted on how to get started with the approach and gave some detailed implementation strategies of the approach. Furthermore, we have highlighted on security awareness metrics, and suggested that for security awareness to be effective it has to be made part of the organisational culture. Finally, we have attempted to outline the validation of the DAISA approach.
Chapter 7

CONCLUSIONS

This chapter concludes the thesis. It discusses the validation of the research and presents a summary of contributions. Then it gives concluding remarks and finally it proposes related future research work.

7.1 Validation of the Research

In Chapter 1 it was clearly stated that both qualitative and quantitative methodologies were applied in this work. This means that personal involvement in the study field, the use of interviews and personal observations data gathering methods suggests a qualitative research Lincoln and Guba (1985); Agostinho (2004); Shulman (1997). On the other hand the use of questionnaires to quantify some of the research findings suggests the quantitative research Neuman (2004); Levy and Lemeshow (1999). In view of this, we shall attempt to assess the validity of this work first with respect to the pre-stated purpose of the research, and then against the grounded criteria for assessment of a qualitative research.

Validation with respect to the purpose of the research

As stated in Chapter 1, the primary purpose of the research was to develop an integrated security education, training and awareness learning continuum for developing countries. However, education and training aspects of the learning
CONCLUSIONS

continuum were accomplished in phase 1 of the research Casmir (2003). In cycle 2 of the research we were focusing more on the awareness aspects. We were, thus aiming at developing an approach that will guide developing countries in implementation of information security awareness programs at workplaces; and eventually, raise security awareness among employees in organisations. To that end, we are confident that the proposed DAISA approach, in Chapter 6, suitably meets this purpose. This is due to the fact that the proposed DAISA approach gives high level guidelines that will help organisations (from small to large) to plan, implement and evaluate security awareness programs in a cost effective way. Also, the approach was developed and evaluated in collaboration with the stakeholders in the region. According to Grundy and Kemmis (1981) the mutual collaboration element in our methodology makes us conclude that the intended purpose was achieved.

Validation with respect to attributes of a qualitative research

Credibility, transferability, dependability and confirmability taken together may be used to establish the validity of a qualitative research Lincoln and Guba (1985, p.290-299). In other words, these attributes are used as a measure of the trustworthiness in a qualitative inquiry and also to support the argument that the inquiry’s findings are “worth paying attention to” Lincoln and Guba (1985, p.290). “Credibility is an evaluation of whether or not the research findings represent a credible conceptual interpretation of the data drawn from the participants’ original data” Lincoln and Guba (1985, p.296). Transferability is defined as the degree to which the findings of the inquiry can apply or transfer beyond the bounds of the context of study. Dependability is defined as an assessment of the quality of the integrated processes of data
collection, data analysis, and theory generation. Confirmability is defined as a measure of how well the inquiry’s findings are supported by the data collected Lincoln and Guba (1985). Therefore, the validity of this work is also assessed against these criteria.

_Credibility:_ – Do the findings presented in this thesis precisely reflect the reality studied?

Reality is subjective Donnell (1999); Agostinho (2004) and context dependent. Reality is also dynamic especially when it involves people; relationship and interactions among people, people and things they do or believe Lincoln and Guba (2000). Therefore, there could be multiple realities by different constructors within the same domain and context of study Agostinho (2004); Shulman (1997). In this case, it is important to limit the question of credibility within the domain and context of study, especially, when it comes to studying the real world problem such as information security awareness in a developing country. Given the same domain of study and in the same context, we can confidently conclude that the findings presented in this thesis, especially in Chapters 3, 4 and 5, reflect the reality on the ground.

In addition, Lincoln and Guba (1985) argue that “the research interaction should take place with the entity-in-context for fullest understanding”. In support of this argument, this research was specifically done within the context under investigation (i.e. a developing country, Tanzania). The questionnaires whose results are presented in Chapter 4 and from which the DAISA approach is founded, were distributed among and collected from 64
different organisations within the context of study. Moreover, the fact that we conducted face-to-face interviews with various stakeholders in the field coupled with interactive sessions Casimir and Yngström (2003) we had with participants during seminars and short courses adds a significant dimension to the credibility of the results.

Furthermore, the fact that there are at least five international publications (i.e. refereed papers) on the findings of this research presented in Chapter 5 is another evidence for the credibility of the findings.

Transferability: – Are the research findings useful to others in similar environments?

Issues of transferability are very sensitive when it comes to research findings. Much as we concede that the findings in this thesis reflect the reality on the ground, we cannot dare to generalise that they are universal in all contexts of developing countries. Findings in this research are tailored to the realities of Tanzania as a case study, specifically, at the time of this particular study. It is, therefore, important here to clearly point out that the findings of this work should not be interpreted as universally reflecting the realities of all developing countries. However, countries with environments similar to ones described in this thesis can easily adopt and use these findings with relatively minor modifications. To establish the actual security education and awareness requirements for a given country, a different study may be conducted. Nonetheless, we strongly believe that findings presented herein and conclusions made from this study might be of use to other researchers and
security educators, especially, in countries with situations similar to that of Tanzania.

*Dependability:* – Could the results be repeated if the study was replicated?

Dependability is to social science what reliability or replicability is to natural science Lincoln and Guba (1985). It is, therefore, extremely difficult to replicate results of a qualitative research Agostinho (2004) even if one applies the same data collection techniques and methodology to the same study area Lincoln and Guba (2000). This is because the reality of the real world being studied changes with time, changing technology and cultures Shulman (1997); Lincoln and Guba (1985); Agostinho (2004). One way to determine dependability for this work could be auditing the data presented against the sources, reanalyse them to get new results, finally compare and contrast against the findings in this thesis. However, the integration of our research methodology (i.e. action research) Stringer (1999); data collection techniques (questionnaires, interviews, seminars, courses, focus group, desk research, and observation); data analysis methods used; and the fact that this research is firmly grounded on systems theory Taschdjian (1975); Bertalanffy (1968); and cybernetics Scrivener (2002) stands to reason for the dependability of the findings.

*Confirmability:* – Do the data help confirm the findings and lead to the implications?
Confirmability is rather a difficult criterion to address Agostinho (2004) as it depends much on the objectivity of a researcher Lincoln and Guba (1985). To this end, we suggest that for confirmability of data one should focus on the logical soundness of the data presented and the reasoning for conclusions drawn rather than focusing on the objectivity of the researcher. In addition, confirmability of the findings can also be tested based on previous criteria such as dependability and credibility. Likewise, since adequate description of the research context has been given and by allowing for responses from the constructors of the multiple realities (i.e. questionnaires results, comments from conferences and from local stakeholders) we can confidently conclude that the data confirms the findings, hence the implications.

Additionally, our findings in and conclusions of this thesis are more of the constructivist view Lincoln and Guba (1985) rather than the positivist view Newstetter (2001). This is because we believe security problems should be addressed holistically Yngström (1996); and according to Newstetter (2001) “the constructivism is holistic and idiographic (descriptive)”. Table 7.1 illustrates the five axioms of naturalistic inquiry Newstetter (2001); Lincoln and Guba (1985). We were attempting to investigate the real problem of security education and awareness in developing countries. This is a reality, which is essentially, subjective Donnell (1999). It draws much on our experience in the field of study (historically, culturally, and experientially). According to Lincoln and Guba (1985) “there are as many realities as there are people”. Thus, data presented in this thesis confirms the findings and leads to the implications based on the people interviewed; participants in the seminars.
and courses; respondents to the questionnaires; and our personal experience in the field.

Table 7.1: Five Axioms of Naturalistic Inquiry: Positivist View vis-à-vis Naturalist View
[Source: Newstetter (2001)]

<table>
<thead>
<tr>
<th>Positivist view</th>
<th>Naturalist view</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single reality exists that is can be empirically observed, fragmented into</td>
<td>Reality consists of multiple constructed realities that can be understood to some</td>
</tr>
<tr>
<td>variables and processes, predicted and controlled.</td>
<td>extent but cannot be predicted or controlled.</td>
</tr>
<tr>
<td>The inquirer and the object of inquiry are separate, discrete entities.</td>
<td>The inquirer and the object of inquiry interact and influence each other, so they</td>
</tr>
<tr>
<td></td>
<td>are inseparable.</td>
</tr>
<tr>
<td>Most actions can be explained as the result of a cause that precedes the effect</td>
<td>Identifying cause from effect is impossible because all entities simultaneously shape</td>
</tr>
<tr>
<td>temporally or simultaneously.</td>
<td>each other.</td>
</tr>
<tr>
<td>Inquiry aims to develop a homothetic body of knowledge in the form of</td>
<td>Knowledge can only be described ideographically as a working hypothesis that describes an individual case</td>
</tr>
<tr>
<td>generalizations that are “true” and will hold for other times and places.</td>
<td></td>
</tr>
<tr>
<td>Inquiry is value-free and maintained as such through use of objective</td>
<td>All inquiry is value-laden. values, paradigm, theory, context, value-</td>
</tr>
<tr>
<td>methodology.</td>
<td>resonant/dissonant</td>
</tr>
</tbody>
</table>

7.2 Summary of Research Contributions
As discussed in Chapter 1, the main contribution of this thesis is the Dynamic and Adaptive Information Security Awareness (DAISA) approach. The approach is an integral part of the lifelong security learning continuum. The DAISA was systematically developed using a scientifically grounded methodology, action research McCutcheon and Jung (1990). The methodology is firmly founded on the General System Theory Bertalanffy (1968); Ackoff (1971) and Cybernetics Wiener (1948). The approach is in itself a contribution
in that it outlines high level guidelines for planning, implementing, and managing information security awareness at workplaces. The DAISA approach is for free and publicly available to any interested organisations. It also encourages in-house capacity building for security awareness. The approach is not biased to any proprietary businesses. These attributes make the DAISA approach more suitable to most of the developing countries that are characterised by scarcity of financial resources. It requires organisations to treat information security (including security awareness) as one of the major priority areas during corporate planning. The approach is dynamic in that it is flexible to keep pace with the fast changing field of Information Technology (IT). In addition, the approach is adaptable to the changing business environments. Together with the main contribution, there come other associated contributions as follows:

**To Business Organisations**

Business organisations that have been long awaiting a professional guide on the planning and implementation of security awareness programs at workplaces, here is the guide. Although it is apparently targeting organisations in developing countries, the approach can equally be adopted in any organisation elsewhere. This guideline is offered free of charge. It is a self-teach guideline to any interested entity. The thesis will be uploaded on the net for online access from anywhere around the globe. Also, the guide will serve as a basis not only for decision making but also for accounting on expenditures on security.
To Governments
Governments, especially in developing countries, like other organisation shall be able to adopt the approach to raise security awareness of their employees in efforts to protect their information assets and critical infrastructures supporting it. This will not only protect governments’ information assets but also build trust and confidence of citizens when accessing government information online such as E-Government Services. Also, since most governments are relatively slower to adopt new changes through their bureaucratic procedures as compared to private business organisations, they should be able to learn from early adopters of the approach, i.e. private organisations.

To IT Managers and Systems Administrators
Systems administrators and IT managers who were facing difficulties in persuading their managements to support security initiatives, the DAISA approach is a handy tool for the task. Using the DAISA approach as a guide they will be in a position to build the business cases around security awareness and confidently present it to the management for scrutiny and endorsement.

To the Research Community
As stated earlier in this thesis there have been fewer, if not none, publications with respect to information security awareness (and security at large) in developing countries. We, therefore, believe that this research will trigger or prompt for many more related research activities elsewhere in developing countries. This work also, shall provide other potential researchers in the area with a comparative base of their findings.
**To Individuals**

Individuals who happened to attend one or more of our courses or seminars have benefited. This is another contribution of this research. In addition, all presentation slides; course materials; newsletter articles; and the Licentiate thesis are available online for everyone’s access. Moreover, this thesis shall be uploaded to the University of Dar es Salaam web site for public access. This way many other individuals will benefit from this research, hence wider outreach, which is one of the objectives of this research.

**To the General Public**

Many (in developing countries and elsewhere) will have free online access to this thesis. This means that its outreach shall be as wide as possible. Thus, many people will benefit from the findings and subsequent implications of this thesis, hence raise their security awareness.

Outputs of phase 1 of this research coupled with the DAISA approach form an integrated information security education, training and awareness learning continuum. The resulting security learning continuum is considered as the overall contribution of the research. The integrated academic and on-site learning continuum, we believe, is the most effective approach not only because it was ranked high by the critique group but also the two do not conflict; and more importantly they complement each other.
7.3 Conclusions

In conclusion, we wish to say that this is the research output of its kind in developing countries. We did not have some previous work done in similar environments to compare with. In this case, findings and subsequent implications may, perhaps, slightly differ if and when a similar research is done elsewhere in a developing country. Certainly, differences in the findings are inevitable since the technology is changing, contexts are different, and business environments are also dynamically changing; refer to the Systemic-Holistic Model in Chapter 2 Yngström (1996). Thus, we urge other researchers elsewhere to carry out related research for enhanced outcomes. Taking the analogy of the old adage that says ‘it takes a thief to catch a thief’ we expand on this maxim by saying that one needs to think like an attacker to be able to control attacks to information assets. This is also in accordance with Ashby’s Law of Requisite Variety, which states that: The variety in a control system must be equal to or larger than the variety of the perturbations in order to control. It implies that only variety can destroy variety. In this case:

_The most effective way to protect your information assets is to think like an attacker, think holistically – but act ethically._

We wind up by the assertion that it is impracticable to attain 100% security using the state-of-the-art technical solutions only neither by a comprehensive security awareness program. However, a combination of the two, we believe, is the most feasible option for effective security.
7.4 Suggestions for Further Work

It can be noted that our proposed approach (DAISA) has not considered kids and teenagers who have been mentioned in Chapter 1 as major clients in the Internet cafes. This has remained as a challenge to be investigated by other potential researchers in future. There are increased concerns among parents that their kinds are frequently surfing the net without them (parents) knowing exactly the content they are viewing. One of the parents interviewed once said to the author “they [kids and teenagers] seem highly motivated with the surfing in the Internet, I don’t know why”.

Another, challenge that has remained unaddressed by this work is ‘how to get lawyers understand the language of IT’. Cyber crimes are increasing around the globe Power (2002); Gordon and Ford (2002). This prompts for immediate actions to be taken to educate lawyers on issues related to Information Security (including cyber crimes) to enable them make informed judgements in such cases. The other research topic that we suggest for future is to implement the DAISA model in some organisations and evaluate it empirically.

In addition, researches similar to one in this thesis need to be carried out elsewhere. Findings from such researches should be published for others in the area to learn from, compare findings, and give critique.
REFERENCES


REFERENCES


Casmir, Respickius and Yngström, Louise (2003a). *IT Security Readiness in Developing Countries: Tanzania Case Study*, IN: Proceedings of Cynthia E. Irvine, Helen L. Armstrong (Eds.): Security
REFERENCES


DTI (2004). DTI Education and Awareness Fact Sheet, Department of Trade and Industry, United Kingdom.


REFERENCES


Appendix A: Questionnaire for Evaluation of a Short Course

2001-11-27
Louise Yngström
Respickius Casmir


We would like very much to have your opinion on the course and IT security. Your answer will be treated completely confidential. We will use the evaluation for research purposes only. Thank you very much in advance!

Please circle where applicable.

I am male/female, age……, undergraduate/graduate student on year….., specialisation……

Have you had information on IT security in any of your computer courses before? yes/no
Have you had computer virus in your computer system? yes/no
If you had, what did you do?…………………………
Have you hacked a system? no/yes – a few times/ yes - many times

How did you understand the concept of IT security before the short course?…………………………………………………………………..
What do you think about IT security after this introduction?………………………………………………………………………
Which of today’s topics and presentations did you find most interesting?………………………………………………………………….Why?………………………………
………………………………

Are there some specific things you would like us to mention during the second day of the course?……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………

Note: Please fill-in this questionnaire and return it back to the presenters at the end of a presentation.
Appendix B: Pre-Training Assessment Questionnaire

Pre-Training Assessment Questionnaire

Please feel free to fill-in this pre-assessment questionnaire aimed at meeting your expectations. Note that there is no ‘right’ or ‘wrong’ answer everything you will write is equally valued.

1. What do you expect to learn from this 5-days IT security Training Program:.................................................................
   ........................................................................................................................................................................
   ........................................................................................................................................................................
   ........................................................................................................................................................................

2. Which of the following methods/approaches do you think is the most effective/least effective way for disseminating IT security knowledge in Tanzania? Rank them from 1 to 5 with – 1 ranked as the most effective and 5 as the least effective method.

   □ (a) Seminars and Workshops
   □ (b) Specialised IT Security Academic Program
   □ (c) Security Training at Workplace
   □ (d) All of the above
   □ (e) b and c

   Other specify…………………………………………………………………………………………
   ........................................................................................................................................................................

   Give reason(s) for your best choice:........................................................................................................
   ........................................................................................................................................................................

   Give reason(s) for your least choice:........................................................................................................
   ........................................................................................................................................................................

3. How do you rate the necessity and urgency of IT security Education and Training in Tanzania? Circle only one that you think is applicable.
   a. Necessary but not urgent
   b. Urgently necessary
   c. Not necessary at the moment

   Other Specify:..............................................................................................................................................
   ........................................................................................................................................................................

4. Give any other comment for improvement of the IT security education and training in Tanzania:.................................................................
Appendix C: Post-Training Assessment Questionnaire

Post-Training Assessment Questionnaire

Please feel free to fill-in this post-assessment questionnaire aimed at assessing effectiveness of the program for future improvements. Note that there is no ‘right’ or ‘wrong’ answer everything you will write is equally valued.

1. Did the 5-day IT security training program meet your expectations:
   □ (a) Yes, Completely.
   □ (b) Yes, about 75%.
   □ (c) Yes, about 50%.
   □ (d) Not at all.

Other specify:……………………………………………………………………………….

2. Which of the following methods/approaches do you think is the most effective/least effective way for disseminating IT security knowledge in Tanzania? Rank them from 1 to 5 with – 1 ranked as the most effective and 5 as the least effective method.

□ (a) Seminars and Workshops
□ (b) Specialised IT Security Academic Program
□ (c) Security Training at Workplace
□ (d) All of the above
□ (e) b and c

Other specify……………………………………………………………………………….

Give reason (s) for your best choice:………………………………………………………

Give reason (s) for your least choice:………………………………………………………

3. How do you rate the necessity and urgency of IT security Education and Training in Tanzania?
   Circle only one that you think is applicable.
   a. Necessary but not urgent
   b. Urgently necessary
   c. Not necessary at the moment

Other specify:……………………………………………………………………………….

4. Give any other comment for improvement of the IT security education and training in Tanzania:……………………………………………………………………
Appendix D: Questionnaire for Evaluation of Information Security Practices

Please take a couple of minutes to fill out this **confidential** survey questionnaire. The results will be used for research purposes **only**.

1. How often do you access a computer and/or network?
   - On daily basis
   - At least once a week
   - At least once a month
   - Other, specify ...............................................................

2. Where do you access a computer?
   - At work
   - At home
   - Both at work and home
   - At Internet café
   - Other, specify ...............................................................

3. Do you think data and information in a computer are important assets?
   - YES
   - NO
   - Not sure
   - Other, specify ...............................................................

4. Do you think it is worth to protect data and information in computer systems?
   - YES
   - NO
   - Not sure
   - Other, specify ...............................................................

5. Have you ever heard/read anything about information security?
   - YES
   - NO
   - Other, specify ...............................................................

6. If you have responded, “**YES**” to question #5 above please mention through which media?
   - Newsletter/Journal
   - Internet
   - Radio/TV
   - Other, specify ...............................................................

7. Do you know what information security is all about?
   - YES
   - NO
   - Not sure

8. How do you view/perceive information security?
It is a technical issue
It is a non-technical issue
It is both technical and non-technical issue
Not sure

9. Ever you attended to any information security training?
   □ YES
   □ NO
   □ Other, specify .................................................................

10. If you have responded, “YES” to question #9 above please mention which training?
    □ Seminar/workshop
    □ Academic program
    □ Conference
    □ Other, specify .................................................................

11. Which category is your organisation?
    □ Private/NGO
    □ Governmental
    □ Academic/Learning Institution
    □ Other, specify .................................................................

12. Does your organisation have a Local Area Network (LAN)?
    □ YES
    □ NO
    □ Not sure
    □ Other, specify .................................................................

13. Does your organisation have at least one computer with access to the Internet?
    □ YES
    □ NO
    □ Not sure
    □ Other, specify .................................................................

14. Does your organisation have a written Information Security Policy?
    □ YES
    □ NO
    □ Not sure
    □ Other, specify .................................................................

15. If you have responded, “YES” to question #14 above are all employees aware of the policy?
    □ YES
    □ NO
    □ Not sure
    □ Other, specify .................................................................

16. If you have responded, “YES” to question #15 above how is the policy communicated to employees?
    □ During orientation program
17. Does your organisation have any formal and regular information security awareness training program?
   - YES
   - NO
   - Not sure
   - Other, specify ..............................................................

18. If you have responded, “YES” to question #17 above whom does the program target?
   - All employees
   - Only IT staff
   - Not sure
   - Other, specify ..............................................................

19. If you have responded, “YES” to question #17 above how often is the program offered?
   - At least once a week
   - At least once a month
   - Yearly
   - Not sure
   - Other, specify ..............................................................

20. Does your organisation have a computer/network security unit?
   - YES
   - NO
   - Not sure
   - Other, specify ..............................................................

21. Does your organisation have a computer incident response plan?
   - YES
   - NO
   - Not sure
   - Other, specify ..............................................................

22. Does your organisation have a computer disaster recovery plan?
   - YES
   - NO
   - Not sure
   - Other, specify ..............................................................

23. Does your organisation have well-documented Backup Procedure for its data?
   - YES
   - NO
   - Not sure
   - Other, specify ..............................................................

24. Does your organisation have a budget for protecting its information assets?
25. If you have responded, “YES” to question #24 above does the budget also cover training of employees in security awareness?
  ☐ YES
   ☐ NO
   ☐ Other, specify .................................................................

26. Is the senior management of your organisation supportive/committed to information security?
   ☐ YES
   ☐ NO
   ☐ Not sure
   ☐ Other, specify .................................................................

27. Is Security Awareness Training (formal or informal) conducted in your organisation prior to users receiving access to an IT application or IT services?
   ☐ YES
   ☐ NO
   ☐ Not sure
   ☐ Other, specify .................................................................

28. Are you aware of any threats, risks and vulnerabilities to your organisation’s information assets?
   ☐ YES
   ☐ NO
   ☐ Not sure
   ☐ Other, specify .................................................................

29. Have you ever encountered a computer virus attack in your organisation?
   ☐ YES
   ☐ NO
   ☐ Not sure
   ☐ Other, specify .................................................................

30. Had your organisation’s computer system ever been attacked or compromised?
   ☐ YES
   ☐ NO
   ☐ Not sure
   ☐ Other, specify .................................................................

31. Do you think information security awareness is a problem/challenge that needs to be addressed in your organization?
   ☐ YES
   ☐ NO
   ☐ Not sure
   ☐ Other, specify .................................................................
32. Are you aware of any laws/policies governing information security practices at a country level (Tanzania)?

- YES
- NO
- Not sure

33. If you have responded, “YES” to question #32 above, please specify……………………

34. Are you aware of any academic institution or any other learning institution teaching information security courses in Tanzania?

- YES
- NO
- Not sure
- Other, specify …………………………………………………

35. Do you think there is a need to establish information security awareness programs at a workplace?

- YES
- NO
- Not sure
- Other, specify …………………………………………………

36. If you have responded “YES” to question #35 above, whom do you think need to be trained in information security awareness at your organisation?

- IT staff only
- All employees
- Not sure
- Other, specify …………………………………………………

37. Do you think there are any threats/risks to your data/information in a computer when accessing the Internet?

- YES
- NO
- Not sure
- Other, specify …………………………………………………

38. Where do you think an attack or a compromise to your data/information in a computer may come from?

- Within the organisation
- Outside the organisation
- Both within and outside the organisation
- Not sure

39. Are all computers in your organisation installed with antivirus software?

- YES
- NO
40. If you have responded, “YES” to question #39 above, is the antivirus software updated on regular basis?
☐ YES
☐ NO
☐ Not sure
☐ Other, specify ...........................................................

41. Are you aware of ‘social engineering’ tricks?
☐ YES
☐ NO
☐ Not sure
☐ Other, specify ...........................................................

42. Do you use the Internet and/or E-mail?
☐ YES
☐ NO

**Gender**  
☐ Male  ☐ Female  
☐ 18-40 Years  ☐ Above 40 Years

*After filling please return this questionnaire to the one who gave it to you.*
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 Wärn, 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 Fähræus, 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

No 05-015 Bylund, Markus
Investigating Game-Based Instruction in ICT Security: an Experimental approach

No 05-012 A Design Rationale for Pervasive Computing

No 05-016 Strand, Mattias
External Data Incorporation into Data Warehouses