A SOCIAL-TECHNICAL VIEW OF ICT SECURITY ISSUES, TRENDS, AND CHALLENGES: TOWARDS A CULTURE OF ICT SECURITY—THE CASE OF TANZANIA

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

Department of Computer and Systems Sciences (DSV), Stockholm University/KTH

Forum 100; 164 40 Kista, Stockholm- Sweden. Tel: +46 8 6747233, Fax: +46 8 703 9025

E-mail: {si-cnt[1], si- jba[2], louise[3]} @dsv.su.se; stewart.kowalski@ericsson.com[4]

ABSTRACT

This paper discusses the human dimension in a 'security chain' within information systems and networks. This dimension is often overlooked at different stages and levels of ICT development and implementation. An example of this omission could happen at the stages of design and implementation of various ICT systems or strategies and policy formulation concerning ICT use; at the level of an organisation or a country as a whole. As a consequence, this human dimension then forms a weak link in the overall ICT security chain. A common insight in this respect is that, a chain is as strong as its weakest link.

A security chain involves coordinated measures both technical and non-technical (social-technical) necessarily taken to enable the provision and maintenance of adequate levels of ICT security within organisations or a nation as a whole. Several studies in the literature have shown that a supportive security culture is an important component in this chain. Security culture encompasses all socio-cultural measures that complement technical security measures. This paper will, drawing on available literature, attempt to identify and characterise the building blocks of a secure ICT environment in an organisation. The identified building blocks consist of: — people, ICT security requirements, ICT security culture, and security systems. Focusing on people, a discussion of the interaction between these building blocks in a social-technical context is provided based on some concepts from specific theories of Organisational Behaviour (OB). The building blocks and their interactions are then organized into a primary model.

In order for an organisation to create, maintain and change its ICT security culture, certain enabling factors and changes at the national level are instrumental and necessary. Taking a social-technical context of Tanzania, the developed model is used to highlight and analyse some of these factors and needed changes in the light of some collected survey data. In particular, the current trends of ICT developments with respect to security and a supporting human capital are analysed. Further, recommendations of future strategies for ICT development in the country with respect to ICT security are also provided. This paper constitutes a part of an ongoing research from which we present some results.

KEY WORDS

ICT security culture, Security system, social-technical model, awareness, knowledge, attitude and behaviours.

A SOCIAL-TECHNICAL VIEW OF ICT SECURITY ISSUES, TRENDS, AND CHALLENGES: TOWARDS A CULTURE OF ICT SECURITY—THE CASE OF TANZANIA

1 INTRODUCTION

The human dimension is an important component in any security implementation effort. Mounting evidence (DTI, 2004; Ernst and Young, 2004) continue to suggest an existence of significant correlations between observed number of security incidents and people's attitude and awareness of security issues. This observation may imply that, the human dimension in ICT security could be fairly addressed by a cultural approach, that is, by instilling a security culture through security awareness, knowledge and skills. This implication conforms to the assertion that, an effective security culture represents one of the necessary foundations for information security management, and cannot be achieved without appropriate attention to security awareness, training and education for all ICT users (IFIP SEC, 2006). The International Federation for Information Processing (IFIP) Working Groups 11.1 (Information Security Management) and 11.8 (Security Education) have dedicated a special workshop session with a theme on security culture, to be held during the IFIP SEC 2006 conference. Additionally, in the recent years themes on security culture have had almost a permanent place in many of the regular security conferences.

For security to be effective, it takes more than having the state-of-the-art technical controls in place. Effectiveness of security depends also on the extent to which every system user understands and accepts the necessary precautions to counter security threats. Literature suggests three key components that should be addressed in any effective security implementation—people, process, and technology (Schneier, 2000). That is; the *people* involved, the organisation of the *process* involved in securing systems/environment and the *technology* used. Security knowledge and skills of people are very important elements as they help them to act appropriately. But security knowledge and skills without an organised environment in which to apply them is mostly ineffective. The same applies to advanced technology; without an organisational framework, it cannot be fully effective. This paper will, drawing on available literature, attempt to identify and characterise the building blocks of a secure ICT environment in an organisation. The identified building blocks consist of: people, ICT security requirements, ICT security culture, and security systems. Focusing on people (human dimension), a discussion of the interaction between these building blocks in a social-technical context is provided based on some concepts from specific theories of Organisational Behaviour (OB). The building blocks and their interactions are then organized into a primary model which can act as 'an organisational framework' showing ICT security culture in relation to other ICT security controls.

In order for an organisation to create, maintain and change its ICT security culture, we take the stand that certain enabling factors and changes at the national level would be instrumental and necessary. Taking a social-technical context of Tanzania, the developed model is used to highlight and analyse the current trends of ICT developments in Tanzania with respect to a supporting ICT security human capital. In the light of some collected survey data, analysis of the current trends in provision of awareness, training and education programmes in key areas of skills formation critical to sustained development of ICT security knowledge/culture in the country is performed. Discussion as regards to the observed situation and recommendations of future strategies are provided. This paper constitutes a part of an ongoing research from which we present some results.

The rest of the paper has the following sections: Section 2—Background and Rationale of ICT security culture. Section 3—Methodology. Section 4—A discussion of issues related to

security culture in a social-technical context. Section 5 –Findings from survey data in relation to ICT security awareness and knowledge. Section 6 –Conclusions; and References are found in Section 7.

2 THE BACKGROUND AND RATIONALE OF ICT SECURITY CULTURE

There exist different definitions relating to the word culture depending on the context of its application. Generally speaking, it refers to patterns of human activity and the symbolic structures that give such activity significance. Different definitions of culture reflect different theoretical bases for understanding, or criteria for evaluating, human activity. Culture, taken in its wide ethnographic sense, is that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and behaviors acquired by man as a member of society (Cohen, 1995).

Relating the definitions above to the context of this paper, the following two concepts are more relevant—*patterns of human activities* and *the symbolic structures supporting them*. Patterns of human activities in this regards are captured by the contemporary global trends where humans are persistently striving to employ ICT in all social-economic-cultural activities. Whereas the corresponding symbolic structures are such as: national ICT policies, ICT infrastructures, general ICT knowledge, specific ICT training programmes, ICT training institutes, and so on. Some of these structures may manifest themselves at the level of an organisation; for example an organisation's ICT policy or organisational culture; whereas other structures manifest themselves at the nation level; for example, the mentioned national ICT policy. Thus, ICT security culture as conceived in this paper has both: *patterns of human activities related to it* and *symbolic structures supporting them*. The focus in this paper is exclusively on *symbolic structures supporting* the ongoing ICT deployments.

Following from the discussion above, it is apparent that culture can be influence by both; factors within an organisation boundary, as well as factors beyond the organisation's boundary. That is, culture is influenced by internal as well as external factors. Before the advent of ICT, it was possible for an organisation to attain security even for information by combining solid/physical access controls, and procedures and processes; as the organisation was regarded as bounded. Unfortunately, this traditional setup of a bounded organisation does not work so well in the current information technology era. This is due to the fact that bounded organisations become unbounded through interconnections and networks. Consequently, the underlying culture of 'security by physical access control' also needs to be changed.

As noted in numerous literatures, cultures are complex and therefore changing them is difficult in most cases (Detert et al., 2000). Within ICT security, culture change involves much more than implementing technology (technical controls) and developing a policy. While technical security controls for ICT systems are critically important (Bishop, 2003; Pfleeger, 2003; Schneier, 2000), they largely depend on the people who operate and come into contact with the systems in their daily duties. The extent to which these, be it systems administrators or regular users, are motivated, knowledgeable, trained, and show willingness in performing their duties with security consciousness makes an important difference. Our focus here is on aspects of motivation, training, skill sets development, and the general knowledge required to foster ICT security culture in organisations and the nation.

The literature holds a lot of information on importance of, and approaches to attain a culture of security with regard to ICT. Example of the available literatures that may be helpful in building a security culture in ICT is the publicised OECD (Organisation for Economic Co-operation and Development) document—Guidelines for security of information systems and networks: towards a culture of security (OECD 2002), which gives high level guideline descriptions for participants at international, national and within organisations. These guidelines constitute a foundation for work towards a culture of security. Conolly (2000) points out that, organisations must have a culture that

makes it clear that security is important; whereas, Verton (Verton, 2000) underlines the importance of security awareness in building organisation's security culture.

Freeman and Wood noted that the body of research is rich in knowledge in the area of organisational security, which addresses aspects such as its construction, and how to improve and maintain it. However, most of the research in this area is focused on certain aspects of security such as security leadership, policy issues, awareness and training, and implementation of specific controls; and not on how these aspects are affected by and could be integrated into, an organisational security culture (Freeman, 2000; Wood, 2000). While these aspects are all very important, their application in organisations requires an existence of some kind of intrinsic support from all participants. This support need to be reflected in, and built upon the organisational culture. Chia argues that the enforcement of an aspect like policy through the traditional cycle of awareness, training, and compliance testing without a supporting culture is likely to be less than optimal (Chia, 2002).

A common theme that can be drawn from the literatures above is that of necessity and importance of security culture in ICT. This necessity seems to be global in nature (OECD, 2002) and it needs the requisite attention at all levels and from all participants (computer systems and networks- users).

The questions here can rather be:

1.) How can participants in ICT meet demands for a sound ICT security culture?

2.) What are the key factors contributing to it?

3.) What are the components of an ICT security culture?

While it is not possible to provide comprehensive answers to all these questions in a short paper like this one, an attempt is made to provide (at least at high level) discussion of key issues with regard to the posed questions. Nevertheless, an obvious general answer for these questions has to do with aspects of awareness and knowledge of ICT security issues as has been revealed in the preceding part of this paper. Also, further relevant and complementing information about culture change and analysis can be found in (Schlienger and Teufel, 2003).

Taking Tanzania as one of the participants in ICT, the current status and efforts (*symbolic structure supporting acquisition of ICT security awareness and knowledge)* towards a culture of security is analysed. This paper can then serve a purpose of country case study and experience towards the goal of global ICT security culture.

3 METHODOLOGY

Being a part of ongoing research, this study is based on primary data sources collected in Tanzania. It is mainly a primary research that involves collection of data (survey data), organising it in some fashion (a social-technical framework) based on some factors (awareness, knowledge, and skills) that we believe are important in fostering ICT security culture. At the level of organizations; six training institutes offering computer/ICT training and education in the country are involved; where their training and education materials/programmes are scrutinized for aspects of ICT security content. Here, the training institutes are regarded as *symbolic structures*. A criterion for selection was to include institutes with training and or educational programmes on computer/ICT. The prime target was on institutes whose programmes are exclusively on computer/ICT training/education. These were complemented by others institutes/university whose curricular include computer/ICT studies in parallel with other fields. At the national level, strategies and policy documents regarding education and training were obtained for reviewing.

The collected data was then analyzed to unveil some trends or pattern, which are then compared against some known examples of good practice in fostering security culture. The primary data sources are, in addition, complimented by secondary data sources from the literature.

3.1 Theoretical basis

A major premise here is based on the belief that, by providing appropriate ICT security knowledge to ICT users, it is possible to internalise security culture. This knowledge could be in the form of education, general awareness of, or specific skills in, ICT security issues. Theoretically, the study is based on the General Systems Theory whereby we view 'system' as one whole (Yngström, 1996), implemented by the social-technical framework (Kowalski, 1994). In a perspective, we view an organization as a social setting with unique cultures, structures, methods and machines. These together can be viewed as constituting a system—*social-technical system*. The social subsystem; has *culture* and *structures* as components, whereas the technical subsystem has *methods* and *machines*. These components are in constant continuous interaction with each other to maintain the system in equilibrium. Thus, changes in any of component or subsystem will tend to effect changes in all other interacting components so as to place the system in equilibrium/disequilibrium.

From the General Systems' theory point of view, *fig. 1* shows a social technical system whereby ICT is being introduced in the technical sub-system (Machines and Methods). Following this change, transformations need to take place in order for the system to accommodate the changes brought about by the newly introduced ICT and once again maintain itself in equilibrium. This study has focused on these transformations from a systems' security point of view. The overall goal is to study, analyze and establish the systems' security readiness requirements taking into consideration the pertinent social-technical states. For the purpose of this paper, an analysis of an aspect of *structures* in the social subsystem—training and education modules targeting ICT security, is on focus.

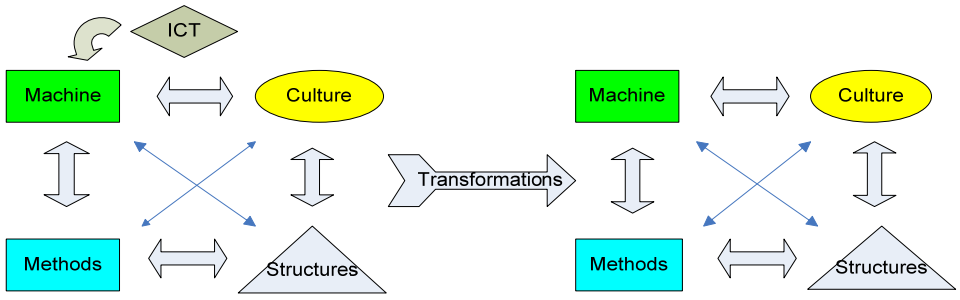

Figure 1: Social-technical system (Kowalski 1994)

4 SECURITY CULTURE ISSUES IN A SOCIAL-TECHNICAL CONTEXT—A DISCUSSION

This section attempts to draw a big picture of ICT security culture in a social-technical context and highlights issues pertaining to the possible answers to these questions: "*How can participants in ICT meet demands for a sound ICT security culture? What are the key factors contributing to it? What are the components of an ICT security culture?"* posed earlier.

Generally, cultures are based on a set of shared underlying assumptions about reality (Robbins, 2003). Here our reality is to attain ICT security in a social-technical system (see fig.1). Culture has effects on attitudes and belief, which in turn play part in individual behaviours—actions and/or reactions. Thus, there is a prime need to determine what attitudes and beliefs need to be cultivated in an organisation, how these manifest themselves in the behaviour of the concerned people and how desirable attitudes and beliefs can be imprinted into formal operational methods to produce the desired outcomes—secure systems, networks, and operations. Thus behaviour needs to be influenced in some ways.

We would like to borrow knowledge already available in other fields in relation to behaviours and attitudes. To this effect, we have found a number of relevant theories from the field of

Organisation Behaviours (OB). Mounting evidence from research in OB (Robbins, 2003) has shown that it is useful in developing people skills; the same should be true for ICT security skills. It is further claimed that actually OB is capable of providing means to explain, predict, and control human behaviour.

Some of the basic theories in OB which could influence behaviour are the following: ***motivation theories***—basically, people are not cold unfeeling machines and hence the theories propose that individuals are motivated to the extent that their behaviour is expected to lead to a desired outcome. Their perception and calculation of situations are filled with emotional content that significantly influences how much effort they exert. Moreover, people who are highly motivated in their jobs are emotionally committed (Robbins, 2003); ***goal-setting theory***— states that intentions expressed as goals can be a major source of work motivation—a potent motivating force; ***reinforcement theory*** – a behaviouristic approach, which argues that reinforcement conditions behaviour; ***law of effect***—behaviour is a function of its consequences and showed that reinforcers (consequences) conditions behaviour and help to explain how people learn.

The law of effect and the concept of reinforcement also help to explain motivation. A large amount of research indicates that people will exert more effort on tasks that are reinforced than on tasks that are not (Stajkovic and Luthans, 1997; Luthans and Kreitner, 1984). Reinforcement is undoubtedly an important influence on work behaviour. What people do on their jobs and the amount of effort they allocate to various tasks are affected by the consequences of their behaviour. Same effect can be produced through goals. This background can equally be used to inform and address the human dimension in security within organisations; as the human dimension in security has to do with behaviours and actions too.

These theories as outlined above point out the following important issues for influencing human behaviour: motivation, goals, reinforcement, and the nature of consequences following an action. In the absence of all these, it seems people may feel themselves being treated as cold unfeeling machines, a condition that could result in adverse effects on behaviours. It is therefore productive if the advantage of these issues can be taken when addressing human issues in ICT security, i.e. to influence the desired behaviours conducive for attaining secure ICT environments in organisations. The desired behaviours would have their roots deep in a vibrant ICT security culture. In order to see how behaviours are related to the overall process of securing an organisation's ICT environment, ICT security culture is placed in a context and then involved actions and issues are outlined. This is the topic of next subsection.

4.1 ICT Security culture in a context: — An overview of parts, relations, and actions

As mentioned earlier, ICT security problems may not always be wholly technical or wholly social but mostly a combination of the two. This combination is realised through the relations and interactions of the social-technical system so formed. Thus, technical solutions alone may not, in the long run, solve the problem. It is from this observation that the concept of security culture finds its relevance in the social aspects of security. Here we attempt to characterise the parts and relations.

According to a common view, information and communication security can be expressed using the three concepts of confidentiality, integrity, and availability. In practice these are afforded through technology, management, and social elements. Technology elements may involve a combination of cryptography, intrusion detection systems, access control mechanisms, firewalls, antivirus, and so on (Pfleeger, 2003). Management elements can be access control policy or a general security policy, procedures and practices. Social elements involve, in addition to the management elements,—ethical/cultural, and legal/contractual issues (Kowalski, 1994). These elements can be grouped into two major categories of technical and social controls.

The actions involved in the process of securing an ICT system requires the knowledge of the possible risks pertaining to the systems, available countermeasures or controls and how to

holistically address them. This may involve analysing the ICT system in question—profiling the would-be adversaries—their intentions, attitudes and characteristics i.e. thinking like hackers; designing countermeasure e.g. developing a security policy, implementing access controls mechanisms, physical protection, and supporting procedures. Normally, this is constructed in layers—deterrence and prevention; protection; detection and containment; and recovery. These layers of controls are hereby denoted as a *security system* and are expected to work harmoniously. A *security system;* is made up of a threat profile from a risk analysis, corresponding countermeasures and needed structures (technical and non-technical)—e.g. secure hardware and software, policies, processes and procedures; (but these lower level details will not be covered here).

However, a *security system* can only be effective not because of its comprehensiveness but also due to the attitudes and behaviours of the people that interact with the system. Thus, the actions of these human elements determine whether the information system in question will be reasonably secured or insecure (assuming a perfect *security system*). This makes *people* an important part of the security system and the OB theories discussed earlier have relevance here. For example, imagine an organisation has in place a good *security system* with a policy that stipulates that all sensitive information from the organisation must be sent encrypted. However, since not all information may be sensitive at any given time, then the system must also have a capability of sending insensitive information unencrypted (in clear). Then, through the actions of a person (attitude and behaviour), this capability can also be used to send sensitive information unencrypted as well, and thus renders the encryption security function ineffective. As attitudes and behaviours are the direct product of the pertinent culture, then cultivating a desired *ICT security culture* is just as important as having in place the right technical controls. Thus, *security culture* is equally an important part of the whole.

The overall range of *security requirements* for an organisation determines the nature of *ICT security culture* that is to be cultivated. In addition, the same *security requirements* determine the policy and types of countermeasures (*security system*) to be implemented. Furthermore, the *security requirements* impose demands on the *people* who would interact with the system. The issues of motivation, training and education outlined earlier are important here also. These different parts or building blocks and relations are shown in *fig. 2*.

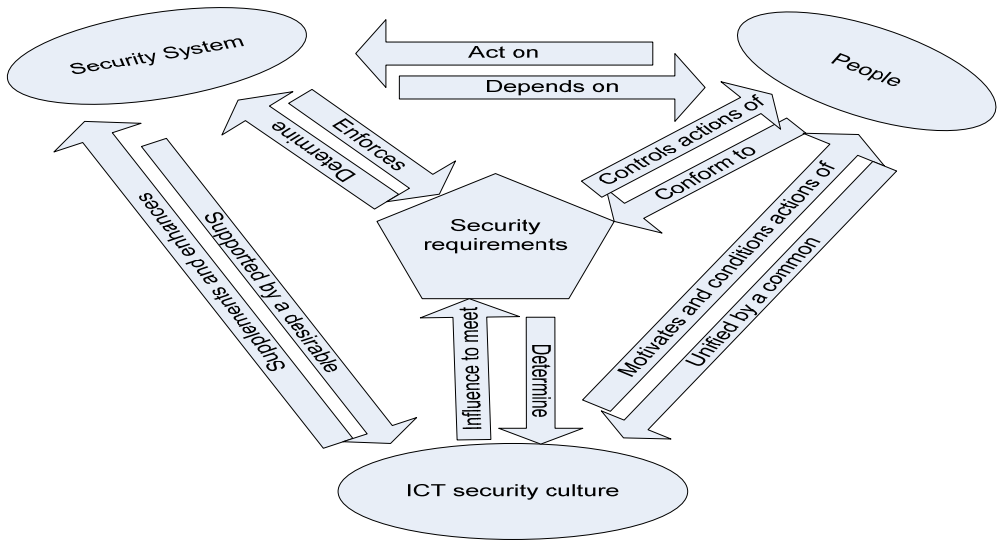

Figure 2: An organisational framework showing ICT security culture in relation to other ICT security controls.

The main issue in focus in this discussion is the behaviour of people. If there could be a method to understand and predict the behaviour, then it's more likely it could also be controlled. As discussed earlier in this paper, at least we have seen OB theories may provide mechanisms for influencing human behaviour. A number of methods can be used to achieve this; such as effective leadership, adequate planning, setting goals, motivating, enforcing responsibility and liability, continuous awareness programs, security education, and imparting security skills.

Cultural aspects in the *fig. 2* can be divided into *security culture mechanisms* (management, policies, personnel, and training and education); *principles and values* (responsibility, honest, integrity, ethics, commitment, compliance, leadership, and motivations), and *shared underlying assumptions* (knowledge of threats and vulnerability in systems, trust relationships, beliefs, and possible malicious acts). These aspects can be realised by breaking the framework, *fig. 2*, to the next lower level to see details of the components; for example the details of the contents of *security system* provided in the discussion above.

Referring to *fig.2*, insecurity in the ICT environment of an organisation could then be as a result of a flawed security system or security requirement specification. Insecurity could also be caused by unwanted actions taken by people due to the absence of a security culture or lack of awareness and knowledge of security issues. As mentioned earlier in this paper, for security to be effective, it takes more than having the state-of-the-art technical controls in place. Effectiveness of security depends also on the extent to which every system user, understands, and accepts the necessary precautions to counter security threats. A security aware culture is one whereby users are aware of the security issues that pertain to their environment, and are knowledgeable and skilled enough to act appropriately.

Thus, based on *fig. 2,* a culture that perceives ICT security to be a technical issue is unlikely to be effective; as in effect, it would only be benefiting from the effects of the *links* and *relations* between the *security system* and the *security requirements*, while missing the-all-important other links and relations shown in the figure. Here, it's where ICT security is represented in a simple equation which says: "ICT security = firewall, or intrusion detection system, or an antivirus, or a combination of the three". Worse still, is where the ICT security in an organisation has a clear and single owner—belongs to IT department! It would also means that this is not an issue that concerns the organisation's top management; their support, which is needed for enforcement of policies, allocating budgets, training, etc., will be missing and hence the whole effort turns out futile.

The culture that tends to address the ICT security problem in an ad-hoc and reactive manner is ineffective, at best; as it misses the big picture as captured in *fig. 2*. Here it's where an organisation responds to security only when there has been a major catastrophe to its processing/IT systems; e.g. an unavailability of systems following a virus outbreak or other possible risks in ICT. In addition, due to lack of proper planning, and the entailing limited and constricted view of the security problem, it's unlikely that the organisation would have a security policy to guide its security efforts; or a proper security awareness and training programmes for its employees/users; which, as discussed earlier, are important in creating and instilling a desired ICT security culture in the organisation and among the employees.

Consequently, the human element in the overall effort of creating a secure ICT environment in an organisation needs to be given the priority it deserves. Desired attitudes and behaviours with regard to security, expected to be displayed by the *people* interacting with information system needs to be cultivated—through awareness and knowledge, motivated, and encompassed within an overall organisational culture; for which a *security culture* could be a subculture. The proposed framework (fig.2) could be helpful in viewing the big picture—a 'whole, with its parts and relations.

In order for an organisation to create, maintain and change its ICT security culture, we take the stand that certain enabling factors and changes at the national level are instrumental and necessary. As discussed in section 2, culture is represented by—*patterns of human activities* and *the*

symbolic structures supporting them. Further it was revealed that these two aspects could manifest themselves at different levels and contexts. Beyond an organisation level, is a national level; and in relation to this, the corresponding *symbolic structures* are such as; national ICT policies, ICT infrastructures, general ICT knowledge, specific ICT training programmes, ICT training institutes, and so on. Following from our stand, a high-level investigation of the extent to which ICT security awareness and knowledge is being addressed in the social-technical context of Tanzania was performed in a search for further insight into understanding the factors effecting the human dimension (*people* in *fig. 2*) in security. This is covered next.

5 FINDINGS FROM SURVEY DATA IN RELATION TO ICT SECURITY AWARENESS AND KNOWLEDGE

The colleted data (see section 3) was organised to indicate the status and trends of the training and education programmes that are on the offer to the general public based on vendor-neutral ICT security training and education programmes. The aim was to find out whether the currents trends of ICT knowledge dissemination involves ICT security knowledge, which as we have seen in the preceding sections, is important in fostering ICT security culture.

Two computer training institutes, one university, one institute of technology, and one regional management institute, and one institute of accountancy were included in the survey. The training/education programmes documents were obtained from these and analysed for the patterns described above. *Table 1* shows the mapping of "other" or "non-security" computer/ICT courses/modules offered by the surveyed institutes and university against security courses/modules, i.e. whether they include security modules. A tick in the cells shows what is available for offer at different course levels.

Table 1: Overview of ICT security courses among a full range of other Computer/ICT courses on offer

Course level	Certificate		Diploma		Advanced Dip.		Degree		Postgraduate	
	Others	Security	Others	Security	Others	Security	Others	Security	Others	Security
Institutes										
CT1	√		√		√					
CT2			√		√		√		√	√
IT			√		√					
IM	√	√								
IA	√				√	√				
UN	√						√		√	

Key: CT1 and CT2 are the two computer training institute; IT = institute of technology; IM = the regional management institute; IA= institute of accountancy and UN= university.

5.1 Discussion

As can be seen on the table, there are only three occurrences of courses or modules bearing ICT security issues among the wide range of IT courses offered by the surveyed institutes /university; one at certificate level, one at advanced diploma level and the other at postgraduate level. This is relatively a small proportion, content wise and out-reach when compared to the other courses in computer/ICT represented in the table. While the other ICT courses have almost occurrences in all levels of certificates, i.e. from certificate level to postgraduate when all six institutes are combined; ICT security courses appear only at certificate, advanced diploma, and at post graduate level; and

this is only in two institutes out of the total six. Still, on looking at the details of the ICT course on offer at post graduate level, it turned out to be an intensive short duration course taking only three week to complete. The contents are: "Overview of IT Developments, Security threats, advanced risk assessment methodologies, advanced issues in Network and Data communication security, Risk matrix and control spreadsheets, Formulating IT Security policies and Data protection acts, total computer security and control in an organization. Whereas, the target group is: ccomputer - based information system managers, Data Processing/Operations Managers, Data-base administrators, analysts/Programmers, auditors and End users who are responsive for preventing, detecting and controlling disruptions, destructions, disasters, and un-authorised access to computers and information systems. While this has positive effects, but the fee for the three week course is on the higher side compared to other non-security IT courses. The fee for this one is US$ 1800 compared to, between US$ 100 – 500 for different modules of most of other IT courses at that level and for that duration. This could be another factor strong enough to keep many of the prospective attendees away.

Other IT courses are various and some are based on international syllabus, whereby local institutes run the courses through accreditation arrangements with external universities, mainly in the UK. Examples of courses are: International Diploma in Computer Studies (IDCS), Bachelors in Computing and Information Systems (B.Sc), and International Advanced Diploma in Computer Studies (IAD).

Since there is a low representation in courses on ICT security compared to others, it may imply also that the competency and awareness of security issues in this social-technical context is relatively low. This assertion is supported by the findings of another study on the state of practice ICT security management in organisations in which the studied organisations rated low in many of the key issues required for a sound ICT security management practice (Bakari et al., 2005).

5.2 Challenges

Although there is a policy at the national level; the National higher education policy of 1999, there are still some operational problems and challenges. Demands for personnel with higher education background have been on the increase both from the public and private sectors. There has thus been a mushrooming of training centres and institutes to cater for the increased demand. The mushrooming of such centres and institute appears to have been haphazardly (encouraged) without proper co-ordination and planning.

Tanzania's education system has grown from relatively simple to a complex one. The system has grown from only one higher education institute (a university college) in 1961 to more than 140 tertiary training institutions; out of which about twenty (20) are higher education institutions. However, many of these have been duplicating one another course programmes and awards (NHEP, 1999). This lack of planning and coordination may also explain the observed discrepancy in the course offered in computer/ICT studies. Most of the institutes offering training and education in computer/ICT studies are private; at times they seem to be driven by the prevailing market forces. Hence there are courses that would attract many students, and these will be honoured accordingly. It appears (from the findings) that, on the one hand there are far more people who want to learn how to use computers and acquire skills on how to use different application packages than those who would want to acquire ICT security skills. Yet, on the other hand; due to inadequate planning as generally noted in (Bennell et al., 1999; Rutayuga et al., 2004) it seems no serious attempt has been made to ascertain that the prevailing labour market demands (including skills in ICT security) for both pre- and in-service training are met. Hence the IT/ICT training provision on offer is essentially supply-driven. The lack of personnel and resources to support information security education at colleges and universities can be another reason. For this deficiency, the lack of trained security experts is a result; which also explains the lack of ICT security culture.

Hence there is an obvious need for cultivating and enforcing ICT security culture. This is an issue that calls for participants at different levels within the organisations and the nation if it is to turn out a success.

6 CONCLUSION

This paper has attempted to address the human dimension in the process of developing, implementing, attaining, and managing ICT security in organisations and/or a nation by reviewing and discussing varying aspects related to building a security culture in ICT. Security culture encompasses all socio-cultural measures that complement technical security measures. In connection with this, issues of attitudes, behaviour, actions, and motivation as they relate to security have been analysed by concepts from the field of organisational behaviour. An organisational framework portraying components of a supposedly secure ICT environment in an organisation has been outlined and discussed. The roles of awareness and knowledge of, and skills in - ICT security issues towards a culture of security have been emphasised in the discussion and this was further supported by analysis of some data collected in a primary research conducted in Tanzania.

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

7 REFERENCES

Bakari, J. K., Tarimo, C. N., Yngström, L., and Magnusson, C. (2005) "State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study," icalt, pp. 1007-1011, Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)

Bennell, P., Bendera, S., Kanyenze, G., Kimambo, E., Kiwia, S., Mbiriyakura, T., Mukyanuzi, F., Munetsi, N. Muzulu, J., Parsalaw, W., and Temu, J. (1999) “Vocational Education and Training in Tanzania and Zimbabwe in the Context of Economic Reform” - Education Research Paper No. 28, 122 p.

Bishop, M. (2003) “Computer Security: Art and Science” Addison Wesley Professional: 1st edtn, ISBN: 0201440997.

Chia, P., Maynard, S., and Ruighaver, A.B. (2002b) "Understanding Organisational Security Culture". Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, pages 731-740.

Chia, P., Maynard, S., and Ruighaver, A.B. (2002) “Exploring Organizational Security Culture: Developing a Comprehensive Research model”. IS ONE World Conference, Las Vegas, Nevada USA.

Cohen, Anthony P., (1995) “The Symbolic Construction of Community”. Routledge: New York.

Conolly, P. (2000). "Security Starts from Within." InfoWorld 22(28): 39-40.

Detert, J.R., Schroeder, R.G. and Mauriel, J.J. (2000). A framework for linking culture and improvement initiatives in organizations. The Academy of Management Review, 25(4), 850-863.

DTI (2004) "DTI Information Security Breaches Survey 2004" – Technical report.

Ernst and Young (2004). "Global Information Security Survey".

Freeman, E. (2000). "E-Merging Risks: Operational Issues and Solutions in a Cyber age." Risk Management 47(7): 12-15.

IFIP SEC (2006) - 21st IFIP International Information Security Conference, Karlstad Sweden. (http://www.sec2006.org/ visited last April 23, 2006.

Kowalski, S., (1994) IT Insecurity: A Multi-disciplinary Inquiry, PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm.

Luthans, F., and Kreitner, R. (1984) "Organisational Behaviour modification and Beyond: An Operant and Social learning approach" Glenview, Il: Scott, Foresman.

NHEP (1999) –"Tanzania National Higher Education Policy"

OECD (2002) "Guidelines for the Security of Information Systems and Networks: Towards a culture of Security"

Pfleeger, C. P. (2003) "Security in Computing" 3rd Edn, Pearson Education Inc. Prentice Hall – Upper Saddle River New Jersey 07458; ISBN 0-13-035548-8.

Robbins, Stephen P. (2003) Essentials of organisational behaviour - Prentice Hall, Pearson Education, Inc., Upper Saddle River, New Jersey, 07458.

Rutayuga, A. B., and Kondo, A., (2004) "Reforming Technical and Vocational Education: The Role of NACTE on Assessment and Certification of Technical Education in Tanzania" The 3rd Conference of the Association of Commonwealth Examinations and Accreditation Bodies (ACEAB)- Fiji.

Schlienger, T., and Teufel, S. (2003) "Information Security Culture: From analysis to change" Third annual ISSA - Information Security Conference. Sandton Convention Centre in Johannesburg, South Africa.

Schneier, B. (2000) "Secrets and Lies: Digital Security in a Networked World" Wiley Computer Publishing, ISBN 0-471-25311-1.

Stajkovic, A. D. and Luthans, F. (1997) "A Meta-Analysis of the Effects of Organisational Behaviour modification on Task performance: 1975-95" Academy of Management Journal, pp-1122-49.

Verton, D. (2000). "Companies Aim to Build Security Awareness." Computerworld 34(48): 24.

Wood, C. (2000). "Integrated Approach Includes Information Security." Security 37(2): 43-44.

Yngström, L., (1996) A Systemic- Holistic Approach to Academic Programmes in IT Security, PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm.