AN APPROACH TO ENHANCE ICT INFRASTRUCTURES' SECURITY THROUGH LEGAL, REGULATORY INFLUENCE

Charles N. Tarimo[1], Louise Yngström[2], and Stewart Kowalski[3]

Department of Computer and Systems Sciences (DSV), Stockholm University/Royal Institute of Technology (SU/KTH)

Forum 100, 164 40 Kista, Stockholm, Sweden. Tel: +46 (0) 8 6747233, Fax: +46 (0) 8 703 9025

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

ABSTRACT

As information systems and networks (ICTs) are increasingly used by governments, different organisations, businesses and end-users worldwide, there has been a common interest in promoting the security of such systems through a variety of methods and approaches. This interest is important to address the challenges posed by the potential harm from security failures of the systems to national economies, international trade and the overall participation of individuals in social, cultural, economical and political life.

Given that different countries are in different stages of ICT use and sophistication, it follows that different approaches are necessary to cater for the desired security, that is, approaches tailored to meet local conditions (within a country). Varying obstacles and challenges in attaining ICT security are the result, in part, of the difference in contexts in the environments found in different countries. For instance, contexts found in developed countries are significantly different from those in developing ones. These differences have impacts and influences on the use of ICT in general and on the security of ICT in particular.

In order for a country to put ICT to effective use, it must be 'e-ready' in terms of among other things, the needed infrastructure, human capital, accessibility of ICTs to the population at large, and the existence of effective legal and regulatory framework to cater for the emerging new demands. It may further entail creation of general awareness of the opportunities of ICT as well as in-depth understanding of specific issues related to the use of ICT in society. In this paper a specific issue, ICT security, is viewed through a lens of legal-regulatory framework in the context of a developing country environment. The analysis of the relationships between a legal system and ICT use in general is necessary. Of particular interest here is the analysis of such relationships in terms of ICT security with the goal of investigating the extent to which legal-regulatory framework can be used towards enhancing ICT security. To that end, the paper analyses the varying relationships and effects between society and ICT use, security issues resulting from such use, and the need for and effects of legal-regulatory framework. The context in focus is that of Tanzania, and an approach is suggested that can help to enhance security using legal-regulatory influence.

KEY WORDS

ICT security, ICT infrastructure, Legal and Regulatory influence, Developing world

AN APPROACH TO ENHANCE ICT INFRASTRUCTURES' SECURITY THROUGH LEGAL, REGULATORY INFLUENCE

Charles N. Tarimo[1], Louise Yngström[2], and Stewart Kowalski[3]

Department of Computer and Systems Sciences (DSV), Stockholm University/Royal Institute of Technology (SU/KTH)

Forum 100, 164 40 Kista, Stockholm, Sweden. Tel: +46 (0) 8 6747233, Fax: +46 (0) 8 703 9025

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

AN APPROACH TO ENHANCE ICT INFRASTRUCTURES' SECURITY THROUGH LEGAL, REGULATORY INFLUENCE

1 INTRODUCTION

1.1 Definition

Information and communications technologies (ICTs) is a term which is currently used to denote a wide range of services, applications, and technologies, using various types of equipment and software, often running over telecom networks. ICTs include well-known telecom services such as telephone, mobile telephone and fax. Telecom services used together with computer hardware and software form the basis for a range of other services, including email, the transfer of files from one computer to another, and, in particular, the Internet, which potentially allows all computers to be connected, thereby giving access to sources of knowledge and information stored on computers worldwide.

Information systems security is a vital component of successful implementation and use of ICTs in organisations in a country. Within an organisation, information systems security needs topmost support from the management and should be addressed at all levels of the organisation (Solms, B. and Solms, R., 2004). On the other hand, the overall management of ICT within organisations in some of the developing world countries, for which ICT security forms a part, has proved to be a complex problem as indicated in recent studies (Massingue, 2003; Wanyembi, 2002). Security as such in ICT is a complex issues and a huge body of knowledge has been accumulate through the years in an effort to attain and improve adequate protection to information and its processing infrastructures. As many organisations are becoming increasingly dependent on ICT to perform their core businesses, the reliable functioning of ICT is paramount. Security is a component of reliability, which in practice is hard to address due to: firstly, complexities within the ICT itself—there is a rapid technological development in the field of ICT. A variety of new technical products are introduced continuously. More powerful personal computers are demanded and also provided. A variety of new information systems, which tend to be open and distributed, are developed and implemented. At the same time, there is a tendency towards convergence of different forms of ICT products and content as well as the demand for connectivity and interoperability—as a consequence, the border and scope of information systems are crossing organisations, regions and countries. Secondly, security has both technical and social aspects, which need to be addressed holistically (Kowalski, 1994; Yngström, 1996).

The current trends within ICT is towards globalisation; consequently, each new developed and implemented information system should in one way or another be capable of joining the mainstream global network and be able to participate in the global information economy. An information system in isolation has little value compared to one connected since much of the value of a specific ICT comes from its compatibility with the mainstream global network. This mainstream global network mostly resides in the developed world. As already noted in (Wade, 2002), the general rule is that the value of developing countries ICT is much reduced if it is not compatible with, say, OECD (Organisation for Economic Co-operation and Development) ICT. Thus globalisation is typical of the application of modern ICT.

However, the increased connectivity as a result of globalisation brings with it associated risks along with the above-mentioned value. One of the risks has to do with the security of the ICTs, in that the ICT is now open to a wider variety of threats and vulnerabilities. For a developing country, its general ICT security status can be (and normally is) used as one aspect of the requirement for compatibility to participate in some specific ICT services, say, within the OECD. Hence, the lack of adequate ICT security not only poses a threat to organisations using ICT in a country, but also bars

them from participating in the mainstream global network. Sadly, while most of the developing countries are currently engaged in deploying and using ICT in various sectors within their economies and social services, it appears that not all of them are paying the required attention to ICT security issues. The aspiration for success in ICT use is normally high. For instance, reference to the current National ICT policy for Tanzania (National ICT policy, 2003) could justify this claim. The "Vision" and "Mission" statements of the policy are—Vision: "*Tanzania to become a hub of ICT infrastructure and ICT solutions that enhance sustainable social-economic development and accelerated poverty reduction both nationally and globally"* and the Mission: "*To enhance national-wide economic growth and social progress by encouraging beneficial ICT activities in all sectors through providing a conducive framework for investment in capacity building and in promoting multi-layered co-operation and knowledge sharing locally as well as globally. "* While these statements are true, the current capacity of the needed infrastructure to accomplish them is inadequate. Security is among the components of the infrastructure that must be addressed. Thus, given the critical role security plays in having reliable ICTs, approaches must be developed that can assist in alleviating the situation.

Different approaches to address this will work differently for different countries. It all depends on the actual situation within a particular country regarding ICT use and the way ICT security is addressed, that is, how the interactions between society and technology affect security. An awareness of ICT security issues at a nation level is an important first step. In addition, security education, security policy and a means to enforce it, security design and implementation, practices, procedures, etc., are some of important issues required to be put in place. Further, availability of the necessary security technology, relevant to the environment in focus, is also important. However, the mere existence of these issues may not guarantee security in itself. It is important to remember that 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. Like wise, social solutions alone such as regulations and law may not do in the long run either. Using the Tanzanian case, the paper attempts to highlight and discuss the relationships between the legal system and ICT use with focus on ICT security. The goal of this paper is to investigate the extent to which legal-regulatory framework can be made to work toward enhancing ICT security. Social Construction of Technology systems (SCOT) approach is used as an aid for analysing the varying relationships and effects between the society and ICT use, as well as security issues resulting from such uses. An approach is suggested that may help to enhance security using legal-regulatory influence.

The rest of the paper has the following sections: Section 2, Security in practice—issues and obstacles in a social-technical context; Section 3, Legal issues in ICT use—relations, requirements, and needed institutional changes; Section 4 - the approach suggested. A conclusion is provided in Section 5 and lastly, references are found in Section 6.

2 SECURITY IN PRACTICE—ISSUES AND OBSTACLES

This sections draws upon the body of research into the social construction of technology systems (SCOT). Trevor Pinch and Wiebe Bijker in their paper "The Social Construction of Facts and Artifacts" (Bijker, Hughes, and Pinch; 1989) made a number of useful observations about SCOT. For example, they noted that social groups define which technological issue or "artifact" is a problem to be addressed. These social groups can be homogenous or heterogeneous, and a problem is defined as such only when there is a social group for which it constitutes a "problem." The decision regarding which problems are relevant is greatly influenced by the social groups concerned with the artifact and the meanings that those groups give to the artifact. In addition, specific parts of a technological system may be subject to different functions or meanings by different groups or individuals, and hence a technological controversy is closed through public opinion, not by technically "solving" the issue (Bijker, Hughes, and Pinch, pp. 30– 44). The use of the concept of a

relevant social group is quite straightforward. The phrase is used to denote institutions and organisations (such as military, educational, or some specific business organisations or industry) as well as organised or unorganised groups of individuals. This framework, (SCOT), is adopted here with ICT as an artifact. The aim is to gain a better understanding of the kinds of relationships that may exist in practice between different social groups and ICT use. We use the understanding of the relationships to address the emerging security issues as the information systems infrastructure develops.

2.1 Issues of Security in Practice

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, etc. 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, legal/contractual. These elements can be grouped into two major categories of technical and social controls. However, in practice it is rare to find the whole set of these elements in place at any one time. Referring to the case in focus; results of a recent study on some key organisations deploying ICT as a tool for carrying out some parts of their business processes indicated that technical controls are the ones mostly employed—if at all (Jabiri, B. K., and Tarimo, C. N. 2005). A general analysis of the current scenario of ICT use is presented next. The analysis will help to view the big picture of ICT security issues, which will then be used to suggest a remedy. As implied from the title of the paper, the focus is mainly on the social issues.

In analysing the relationships between different social groups within an organisation deploying ICT in its business processes, a conceptual representation of the organisation is used, (see figure 2.1). In the figure, a conceptual organisation is shown with several departments (Dept1, 2,…), which are joined in function by ICT. Each department represent a social group within the organisation. Since departments are formed based on their functions within the organisation (such as Finance, Administration, Personnel, etc.,), this may imply that the social groups so formed in the organisation are heterogeneous. According to SCOT, these groups will have different meaning for ICT – mostly determined by the way each social group (Dept) uses ICT in performing its functions. In turn this will have implications on the requirements for security in each social group. Hence some social groups would need, say, more confidentiality in performing their activities while others probably perceive availability as what is more important to them as far as security is concerned.

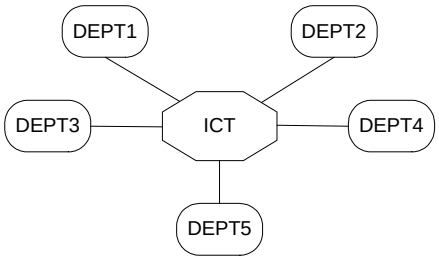

Figure 2.1 The relationship between ICT and the relevant department within an organisation

Security problems with ICT, e.g. infringement of confidentiality or integrity, are indicated for each social group as problems (Problem1, 2,…). In figure 2.2, a conceptual view of a department is shown with its relevant ICT security problems (insecurity). The problems can be those of integrity, confidentiality or availability depending on the actual security requirements. Further, in figure 2.3, a particular problem is isolated and its possible solutions included. These can imply having a security policy in place, using access controls, legal/regulatory, etc. By analysing the nature of a particular problem, several alternative solutions can be identified. However, the kind of possible solutions arrived at would be greatly influenced by a range of social and economic, as well as

technical factors relevant to the environment. The social-cultural and political situation of a social group shapes its norms and values, which in turn influence the meaning given to an artifact. It is from this notion that an attempt is made here to address ICT security by altering a social-cultural situation. As for the technical factors, the features of contemporary technology, in particular the growing importance of industry and public standards and the increasingly configurational character of technologies as assemblages of standard and customised components need to be observed and accommodated by a solution.

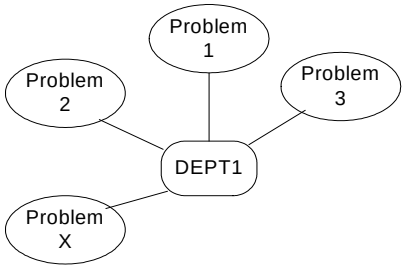

Figure 2.2 Insecurity-Dept relations

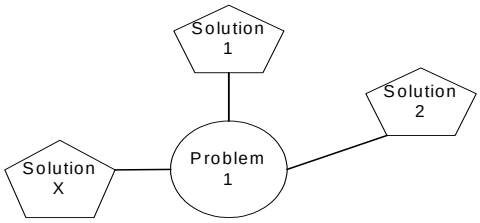

Figure 2.3 Problem-Solution relations

Having analysed the kind of relationships between ICT and its users in a conceptual organisation, we now use the analysis to reflect on the actual situation on the ground [Note: a comprehensive report on ongoing research on ICT developments in Tanzania is found in (Nielinger, O., 2004)]. We aim to examine emerging security issues as deployment and use of ICT captures more ground on the environment. A recent empirical study (Jabiri, B. K., and Tarimo, C. N. 2005) indicates that there is a general laxity in handling ICT security issues. The reasons for the observed conditions are a combination of many issues. Among them are: lack of awareness, budget constraints, and the absence of security policy, procedures, and practices as well as security training. Other reasons were shown to be results of the notion that ICT security is a "specific-department" issue (IT department) rather than an issue for the entire organisation. Worse still, this "specific department" is not furnished with the needed resources to cater for the "big" task under its responsibility – in essence here security means technical controls.

In addition, participants (mostly technical people, such as systems administrators) in one public seminar on ICT security awareness held in 2004 in Dar-es- Salaam aired their views on how they address ICT security in their organisations and the obstacles they normally encounter. The seminar was organized by the Commission for Science and Technology (COSTECH) of Tanzania and was one of several held. Attracted participants were technical people from several organisations and some ministries in the government. Following different presentations on ICT security topics in the seminar, there was an intense discussion and exchange of views. In the end the common view was that security issues are fairly well known to some people in the organizations. However, problems arise when a proposal for funds for a certain ICT security improvement project needs to get up the hierarchy for approval. For instance, through individual initiatives within an organization, a critical security issue might be identified for which funds must be released for purchasing or for catering for the needed inputs. It, most times, gets really difficult to convince the top management of the idea. From the foregoing cases—laxity in handling security issues and lack of enough management support what we can see from our earlier figure on ICT-Department relationships, figure 2.1, is a kind of unstable relationship between departments within an organization and ICT with respect to security of ICT. This implies that, within the same organization, different user-groups will have different security levels—some high, some low, since there is no overall coordination and some department might be more knowledgeable and active towards security (IT department) than others. It is hard for a single department (say, IT department) to address security issues for the entire organization without top management support or enough resources to do so. The fact that Tanzania is in the early stages of ICT development and adoption, the pattern of instability with respect to ICT security as demonstrated here at an organization level

will continue to manifest itself and exist in the emerging infrastructure as can be seen in figure 2.4, below. As a result, the overall structure and architecture of ICT is insecure. The figure shows different information systems coming together as a result of the demand for integration and interoperability of ICTs. The information systems are those of different organizations and may involve both private and public sectors. Some of the social groups (organizations) in the emerging infrastructure are regulated—for example the banking industry. Also within unregulated organizations, a particular social group may be regulated while others are not—for example finance and book-keeping departments. As there is no central coordination mechanism to oversee and regulate how security issues are handled within different social groups as the groups develop and finally integrate their information systems into the growing infrastructure, security stability is hard to guarantee. A weakness in security in any link in the infrastructure affects the whole complex.

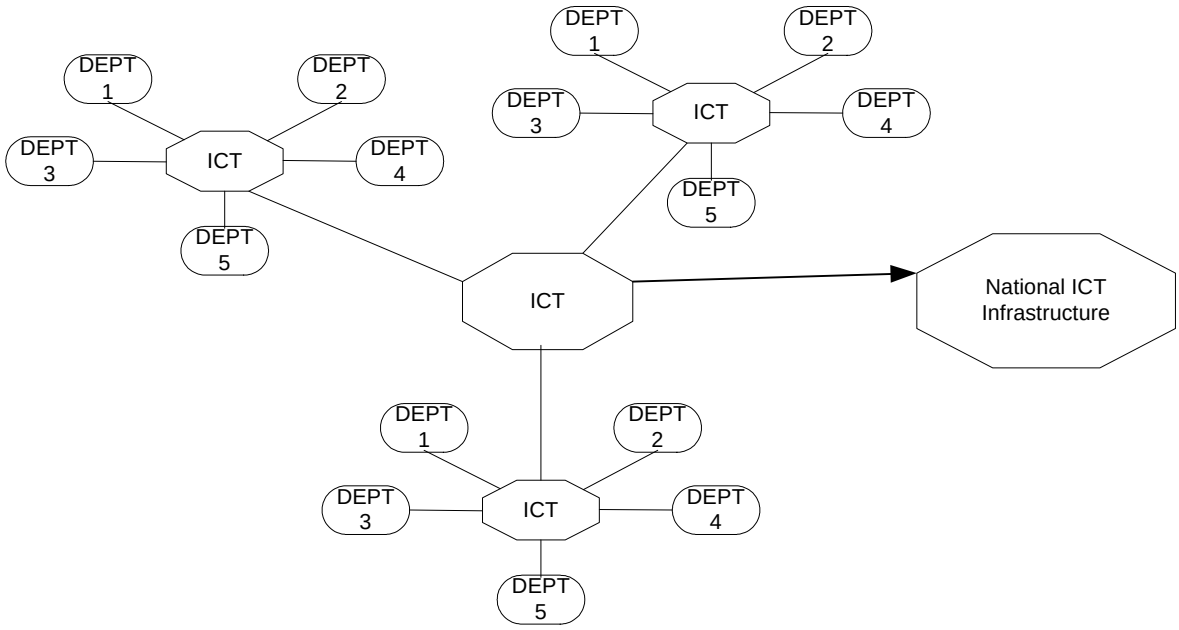

Figure 2.4 The relationship between ICT and different social groups as they join to form the national ICT infrastructure

As mentioned earlier, security must be holistic—involving technology and social elements. Security is not a single feature like a firewall, or intrusion detection system, neither does it start or stop at the computer terminal. As the National Research Council of the USA put it: "security comprises at minimum computer hardware, software, networks and other equipment to which the computers are connected, facilities in which the computer is housed, and persons who use or otherwise come into contact with the computer. Serious security exposures may result from any weak technical or human link in the entire complex. For this reason, security is only partly a technical problem—it has significant procedural, administrative, physical facility and personnel components as well."(NCR 1991, p. 17)

2.2 Obstacles to effective security in practice

Apart from dealing with the more common obstacle such as insufficient budget for ICT security, poor infrastructure and other technology issues in security, we instead pay more attention to the social obstacles to adequate ICT security, such as a regulatory framework. We are working under a premise that although those other factors mentioned above are relevant, still the current level of ICT security is unnecessarily low—meaning it could be improved. Also the current handling of security is not satisfactory—some kind of incentive/push is needed. Findings of research done elsewhere indicate that information security is normally poorly practiced because the liability is so dispersed. A survey on fraud against auto-teller machines (Anderson, R. J., 1994) indicated a correlation between the pattern of fraud and the entity that is liable for the transactions. In the USA, if a

customer disputes a transaction, it is the duty of the bank to prove otherwise; as a result the US banks are motivated to protect their systems properly. On the other hand, in Norway, Netherlands and the UK, the banks are right unless proved otherwise. That means it is the customers' duty to prove that the bank is wrong in a disputed transaction. As probably only a few cases of this kind would succeed, the banks in these countries became careless and fraud kept rising.

The scenario captured above—effects of incentives (liability), resembles the one in focus here where information systems are developed without adequate security as elaborated in this paper—there is no incentive to make security a natural occurrence in the development and deployment of the ICTs in organisations. Here we are concerned with the security of the emerging infrastructure. If we can use an analogy—it is true that anybody with enough money can buy a car, and learn how to drive if (s)he is not yet a driver. However, having a car and knowing how to drive does not sufficiently qualify the person to use the car on a public road. Traffic regulations impose requirements on the owner/driver to have among others a valid driving license and the car itself is to meet some requirements - say those of safety and emission controls - before it can be allowed on public roads. Still, the mere existence of traffic regulations has not been observed to cause a reduction in the number of cars that are bought and put on road. Instead what is observed is more order and safer use of roads. A driver is not only using his past experience in driving and how the car feels as he drives, but also he is constantly influenced in the background by the traffic law. Adding yet another insecure information system on to the infrastructure is equivalent to adding unsafe, polluting cars on roads. This needs to be regulated in just the same way as polluting cars are regulated, but, in ICT context—tailored to the requirements of ICT security. The same kind of influence is needed too. The next section gives a brief outline of legal issues in ICT use—relations, requirements, and needed institutional changes.

3 LEGAL ISSUES IN ICT USE

The legal issues in ICT use are many, and concern the unavoidable changes demanded on existing norms, regulations and legislation as ICT use in society captures more grounds. It is not possible to cover most of them here so a brief overview of some of the relevant issues is presented, mainly from an ICT security perspective. As already noted, institutional changes are necessary as ICT use becomes widespread. Referring to the earlier discussion illustrated by figure 2.4 above— the transition from a simple local use of ICT within an organisation, to nationwide use of complex systems and platforms where ICT plays a major role, would require substantial institutional changes. Although the current status of ICT development and use is not there yet— i.e. nationwide complex systems, the vision is towards there. Hence, necessary institutional changes for efficient and secure development of ICT infrastructure should be made now. Here the interest is on those changes that make it possible for ICT diffusion in society—removing constraints in the law which seem to be against the new ICT, as well as changes in the law that would promote the use and security of ICT. For instance, enacting law to deal with cyber crime creates confidence for online activities such as e-commerce, etc. Consequently the relationship between Law and ICT can be that of acting as an obstacle or an enabler. With respect to security, the law will be an enabler of ICT security when there is a provision in it to prosecute those who compromise security of information systems—hence providing confidence to that part of society which uses ICT for, say, business. At the same time, law acts as an obstacle to those who would wish to compromise systems – i.e. it is deterrent to would-be cyber criminals.

Security and safety may be regarded as aspects of the infrastructure and they touch upon issues such as individual privacy, data protection, redundancy and securing individual computers so that they are not acting as "pollution" agents to the infrastructure. Public use of ICT calls for government intervention through its institutions such as the legal framework. Law must not unnecessarily prevent or complicate the use of ICT. In the national ICT policy (National ICT policy, 2003), provisions are there which call for the creation of a secure cyber-law environment to work with the existing legislation. The call is seen as first priority before any significant new

developments can emerge in ICT related services. Other policy changes have been proposed for a number of sectors such as productive sectors and service sectors. Given the demands for convergence—the phenomena where separate areas such as telecommunication, media, and data processing come together, the need for regulation strategies of some of the emerging aspects from the convergence is crucial. These areas have traditionally been regarded as separate areas of legal regulation. Now, with the converging phenomena, at the minimum, the basic demands for rule of law, information security and personal data protection must be addressed. To quote Seipel, "Information and communication technology is a complex and multifaceted array of elements finding its uses in the most diverse contexts. From the point of view of law this is an essential assertion. Sloppy thinking sometimes seeks to reduce ICT to a simple tool, similar in kind to a saw or a typewriter. The reasoning goes: We don't need a law of typewriters, neither is there a need for a legal theory of saws and sawing. Ergo, ICT is not worth fussing about" (Seipel, 2002).

The present legal framework and related institutional infrastructure of Tanzania is not conducive to ICT development and application as noted in (National ICT policy, 2003). Thus, strategies must be sought for proactive approaches in order to alleviate the situation. Legal reforms must take into consideration both the International legal dimension and the internal (National) legal dimension, as ICT is global and borderless.

Issues in the international legal dimension are mainly for compliance to different international standards and laws in order to foster interoperability of the national legal regime in developing global ICT services such as e-commerce. These include compliance to international agreements/standards relating to ICT such as the EU Directives 95/46/EC on protection of individuals with regard to processing of personal data and on free movement of such data (Directive 95/46/EC, 1995) and the United Nations Commission on International Trade Law (UNICITRAL).

Sector-specific laws also do exist, especially in the US, but their influence impacts almost everyone to some extent. Such laws are: 1) Health Insurance Portability and Accountability Act (HIPAA) passed in August 1996 to improve the portability while maintaining the privacy and security of patient information. This law affects medical providers, insurance companies, claims clearinghouses, etc. Unlike some other laws, HIPAA lists very specific technology standards and policies that must be implemented to comply. 2) Gramm-Leach-Bliley Act passed in November 1999 to protect the information financial institutions collect about customers. This law affects mainly financial institutions, but also any company that collects names, social security numbers and bank account numbers from customers or employees. The act's 'Safeguards Rule' force financial institutions to design, implement and maintain safeguards to protect customer information. With this law, all companies that collect financial information must take security measures, such as maintain firewalls, install and update virus protection, and schedule routine security audits, as well as develop and implement privacy policies. 3) Sarbanes-Oxley Act passed in August 2002 to restore investor confidence in the financial reporting of public companies and hold a company's officers personally responsible for misrepresentation. It affects any public company and is a very broad-sweeping law. Effects on IT departments: Two-phased; initially, companies will struggle just to comply with the law—providing necessary documentation to auditors. Eventually, companies will want to automate the process—building audit trails and procedures into their systems. The foregoing are some of the issues in the international legal dimension.

National legal dimension should address among others, issues of intellectual property rights and convergence/competition—in that where sector-specific, or technology-specific regulation may have been suitable before, the converged nature of technology and services implies a greater reliance on competition policy, law and regulation to guard against abuses of dominance or other anticompetitive behaviour in the marketplace. The object of competition law, however, is not to protect certain actors but to ensure a competitive market by enhancing efficiency to stimulate development. In addition, the national legal dimension should address regulatory reforms in all areas that touch upon ICT services such as e-commerce, infrastructure, etc. This may involve

enacting laws that allow a business to take action against those that breach information security procedures, thus acting as both a deterrent and enabling businesses to recover damages, and other such infringements. Complementary to this is a law that requires of the business that certain security procedures are put in place, generally in order to protect the infrastructure or some third party entity such as a customer. This paper is towards that end—attempting to instigate a regulation on the security aspect of ICT infrastructure.

4 AN APPROACH TO ENHANCE SECURITY BY REGULATION

Following the analysis and discussion covered in this paper, the problems of insecurity in the emerging ICT infrastructure is caused in part by the lack of incentive and overall coordination for adequate infrastructure security to take place as it develops. This has been indicated in the analysis. Influence and coordination form important ingredients towards standardisation. We propose that organisations and any other entities within the country that would wish to develop and deploy information systems for public use, should be influenced by some kind of legal/regulatory force towards observing security in doing so. Since changes in the electronic environment can bring about factual situations that are hard to foresee, legal solutions that were appropriate at a certain stage may become uncertain and/or even disputed and thus prompt a review. Given the current developments in ICT use taking place in the country, order in the development process is important—here from the security perspective, hence to impose constraints and requirements on it may help to shape or re-shape the emerging electronic environment in a legally acceptable way. Consequently if the vision is to use ICT for e-commerce and other online services, then the current ICT infrastructure should develop in such a way as to foster fulfilment of the requirements of the anticipated uses—security being one of the ingredients. In addition, security is needed for other requirements as outlined in section 3 above.

The approach should be to create liability due to failure in security of the ICT to be borne by the owners of the systems, which hopefully would prompt an incentive to deploy sufficient controls. This may involve having specific directives (such as the OECD Guidelines for the Security of information Systems and Networks) and/or enacting security-related laws to correct the perceived imperfections as the ICT infrastructure develops and provide the incentive for organizations to accommodate societal goals such as privacy protection as they perform their businesses. This process should be proactive and dynamic since the electronic environment is changing so rapidly. Periodic reviews should be performed and identified discrepancies addressed. Figure 4.1 below shows a process view of the propose approach.

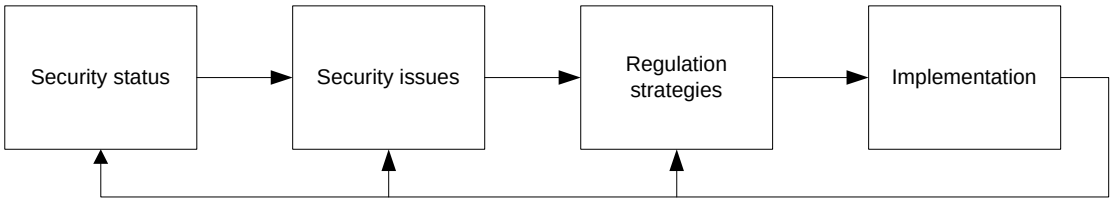

Figure 4.1 Process view of regulatory reform towards ICT Security-regulated environment

Components of the process in figure 4.1 are as follows: Security status is the state of how issues of ICT security are currently being addressed as analysed in parts of section 2.1 above. Security issues are those such as privacy for individuals, confidentiality, integrity and availability of information and processing systems, etc. Given, the actual state of the previous two blocks—security status and issues, a regulation strategy is worked out. Here issues such as what to regulate, how, at what level, etc are considered. Lastly, the strategy is implemented.

The process begins with the analysis of the current situation (status of ICT Security or ICT security-readiness), then in the second stage, various issues regarding ICT use are examined from security perspective such as policies, laws etc. These are used to inform the strategies in the next stage, which in turn lead to implementation. After implementation, (enacted security related law) the effects are observed and through a feedback channel the whole process starts over again. This is in order to take care of the ever-changing electronic environment.

As for the nature of the regulation, a technology-neutral regulation is desired to accommodate changes that take place following technology developments. The current structure of regulation framework in the telecommunication sector is imposed on all licensed services and/or infrastructure, mainly for control and collection of Government revenues. On the contrary, what is proposed here is regulation in order to improve an aspect of the infrastructure—security.

Legislative solutions for ICT have been employed in several countries. In terms of legal issues raised by the need for information security being dealt with through legislative, reviewing Data Protection and Privacy issues will give a clue. Data protection currently exists in several European and other industrial countries. For instance; U.K.: Data Protection Act 1984; U.S.: Privacy Act 1974; France: Data Processing, Data Files and Individual liberties Act 1978 etc. Also there are 44 countries in the world with Penal Legislation for Unauthorised Access to Computer Systems in their Legal Frameworks. Out of the 44 only three are from Africa, namely Mauritius, Tunisia and South Africa (Schjolberg, Stein 2003). In Tanzania, law reform issues are handled by Law Reform Commission of Tanzania (LRCT, 1983). This paper may find use as an input to the Commission when issues addressed here are in focus in their agenda.

5 CONCLUSION

There are many possible ways of solving a problem. What has been discussed and ultimately proposed here is what seemed a likely solution out of many possible. We have arrived at the solution taking into consideration the current state of the ICT development in the country both at the national and organisational levels. Relevant problems as far as ICT infrastructure development is in progress have been analysed and discussed from a social-technical perspective. An approach towards a solution for some aspects of the problems has been proposed—regulatory reforms towards ICT security-regulated environment.

However, it may be a long time (though hopefully not) before such a proposal is put into practice since changes in the legal system often take some time to be effected. This is at the national level where what has been proposed here is designed to take effect. While it is not certain when this is going to happen, it is certain that different organisations will continue to implement and deploy ICTs as shown in section 2 above and probably without adequate attention to security as has been observed if immediate steps to remedy the situation are not taken. Worse still, if there will be no public standards at least for the environment in focus the result would be a catastrophe when the stage comes for the different ICTs to interconnect—convergence. Instead of waiting for the government intervention, organisations deploying ICT can put forward their own initiatives to make sure that their systems follow standards that allow for security, interconnectivity and interoperability with other ICTs in the country and beyond. For instance, the features of contemporary technology, in particular the growing importance of industry and public standards and the increasingly configurational character of technologies as assemblages of standard and customised components need to be observed and accommodated when information systems are developed and deployed.

Thus, analysis of the problem, the proposed approach and the discussion covered in this paper helps at least to show the existence of the problem and a way towards a possible solution. Other alternative solutions can also start from this analysis; hence it provides a staring point for further analysis to take place regarding other issues relevant to ICT infrastructure security, which is in course of development.

6 REFERENCES

Anderson, R. J., "Why cryptosystems Fail" in communications of the ACM vol 37 no 11 November 1994, p. 32—40.

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

Bijker, W.E., Hughes, T.P, and Pinch, T. (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, The MIT Press, Cambridge, MA (1989).

Directive 95/46/EC of the European Parliament and of the Council of European Union, 1995.

Jabiri, B., Tarimo, C., State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study, IEEE – ICALT 2005 (In the Press).

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

LRCT - Law Reform Commission of Tanzania, 1983. Also available at http://www.lrct-tz.org/ [last accessed April 21, 2005]

Massingue, V. S., *Building Awareness and Supporting African Universities in ICT management: The Big ICT Five (Strategy, Development/Acquisition, Implementation, Utilization, Service management)* Doctoral Dissertation, Delft University of Technology, 2003.

Nielinger, O., "Creating an environment for ICT in Tanzania" – Policy, Regulation and Markets, Hamburg Institute of African Affairs, 2004.

OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of Security, 2002.

Schjolberg, S., The legal framework - Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries, 2003. Also available at http://www.mosstingrett.no/info/legal.html#COUNTRIES [accessed on April 21, 2005]

Seipel, P., Law and ICT: A whole and its Parts in Law and Information Technology – Swedish Views, The IT Law Observatory of the Swedish ICT Commission, SOU 2002: 112.

Tanzania National ICT Policy, March 2003. Also available at http://www.tanzania.go.tz/pdf/ictpolicy.pdf [Accessed on April 20, 2005]

UNICITRAL - United Nations Commission on International Trade Law, available at www.unicitral.org [last visited on 21st April.2005]

Wade, R.H. "Bridging the digital divide": New route to development or new form of dependency? In Global Governance, 8(2002), 443-466.

Wanyembi, G. N., *Improving ICT in Public Universities in Kenya*, Doctoral Dissertation, Delft University of Technology, 2003

Yngström, L., *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, 1996.