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

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

Department of Computer and System Sciences

Stockholm University/Royal Institute of Technology

Forum 100, SE-164 40 Kista, Sweden

Tel: +46 (0)8 674 72 37

Fax: +46 (0)8 703 90 25

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

ABSTRACT

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

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

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

KEY WORDS

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

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

## 1 INTRODUCTION

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

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

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

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

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

## 2 METHODOLOGY

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

*Table 1-1: Respondents distribution*

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

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

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

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

## 3 AN OVERVIEW OF ICT SECURITY MANAGEMENT IN THE STUDIED ORGANISATIONS

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

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

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

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

## 4 BENEFITS AND DRAWBACKS OF OUTSOURCING ICT SECURITY SERVICES TO MSSP

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

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

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

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

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

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

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

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

### 5.1 Skills

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

### 5.2 Facilities

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

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

### 5.3 Implementation

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

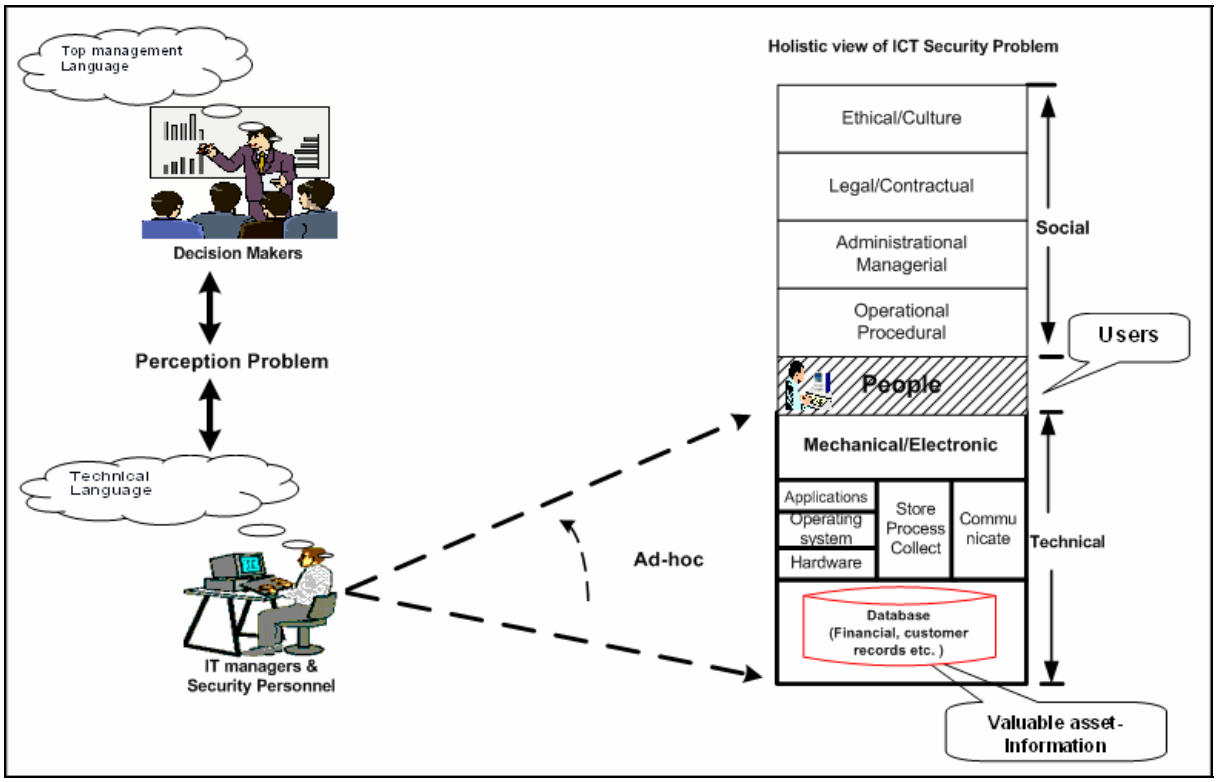


*Figure 1: How the ICT Security Problem is perceived and the way is being addressed*

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

### 5.4 ICT security awareness

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

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

### 5.5 Infrastructure and cost

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

### 5.6 Focus is on the computerisation Process

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

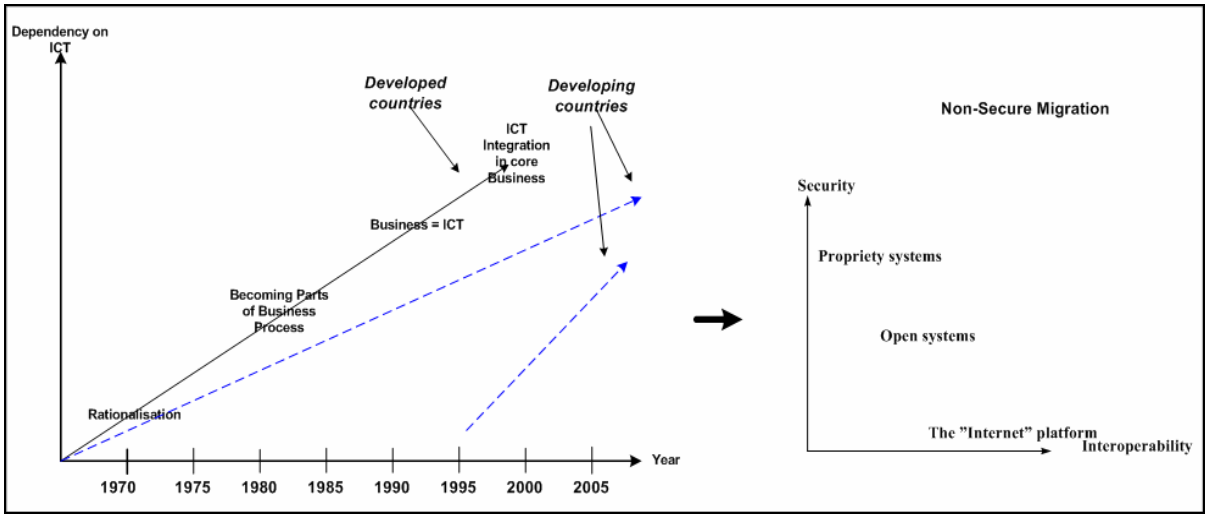


*Figure 2: ICT Integration in Core Business vs Non-secure migration (Bakari, J. K. 2005a; Pg. 61)*

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

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

### 5.7 Sense of ownership and trust

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

### 5.8 Prosecution and other Legal related issues

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

### 5.9 Termination of Relationship

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

## 6 DISCUSSION

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

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

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

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

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

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

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

## 7 CONCLUSION

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

## 8 REFERENCES


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

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

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

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

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

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

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

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

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

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

11. Magnusson, C. (1999). Hedging Shareholders Value in an IT dependent Business Society, THE FRAMEWORK BRITS. *Ph.D Thesis, Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, Stockholm*.

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

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