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

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

Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology, Forum 100, SE-164 40 Kista, Sweden, Tel: +46 (0)8 16 1697, Fax: +46 (0)8 703 90 25, E-mails: {si-jba[1], christer[2] si-cnt[3], louise[4]}@dsv.su.se

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

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

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

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

Key words: ICT Risk management, EMitL tool, Countermeasures

1. INTRODUCTION

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

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

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

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

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

2. METHODOLOGY

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

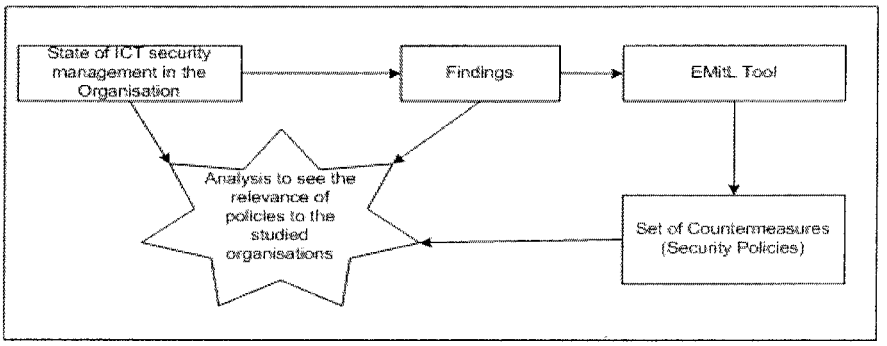

Figure 1. Summarising input and output to EmitL tool

In the next section we briefly describe the EMitL tool.

3. EMITL TOOL

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

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

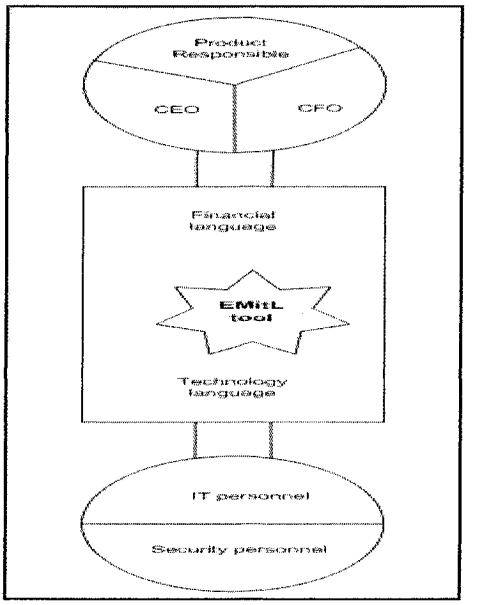

Figure 2. Function of EmitL tool: Source (Magnusson, 1999)

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

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

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

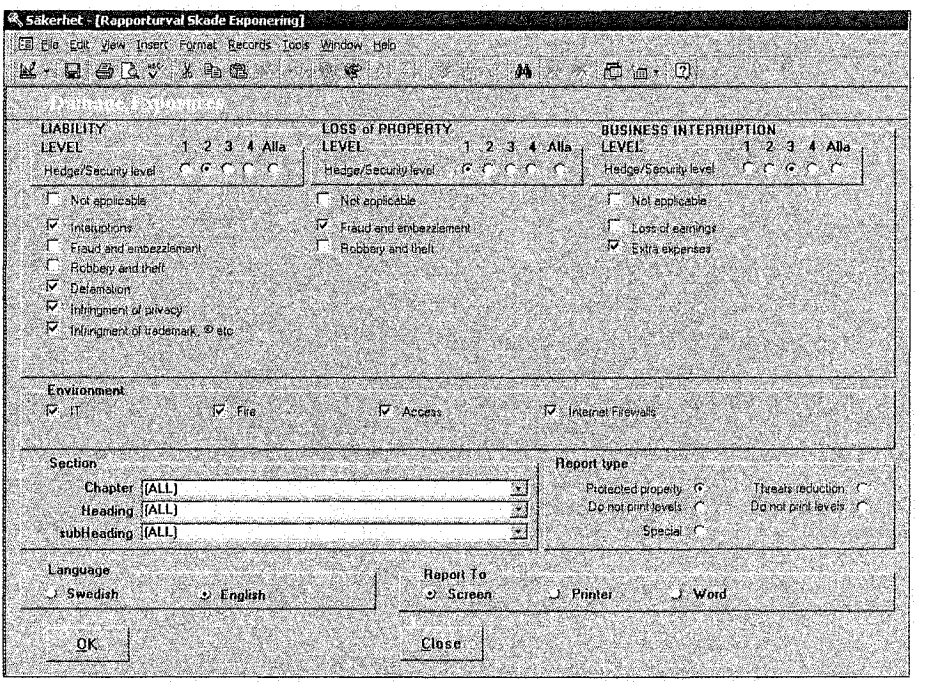

Figure 3. Snapshot of the EmitL tool interface

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

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

Table 1. Damage exposure and ICT security properties

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

Source: (Magnusson, 1999, P. 143)

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

4. BRIEF STATE OF ICT SECURITY IN THE STUDIED ORGANISATIONS

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

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

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

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

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

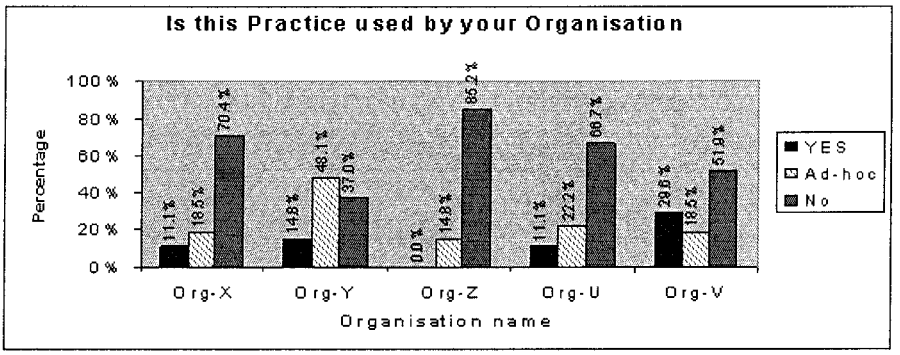

Figure 4. Responses on the countermeasures being practised by organisation

Note:

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

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

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

5. FINDINGS AND DISCUSSION

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

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

Table 3. Damage exposure levels (Security levels)

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

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

Table 4. Showing different input parameters to database EmitL

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

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

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

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

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

5.1.1 Unique measures

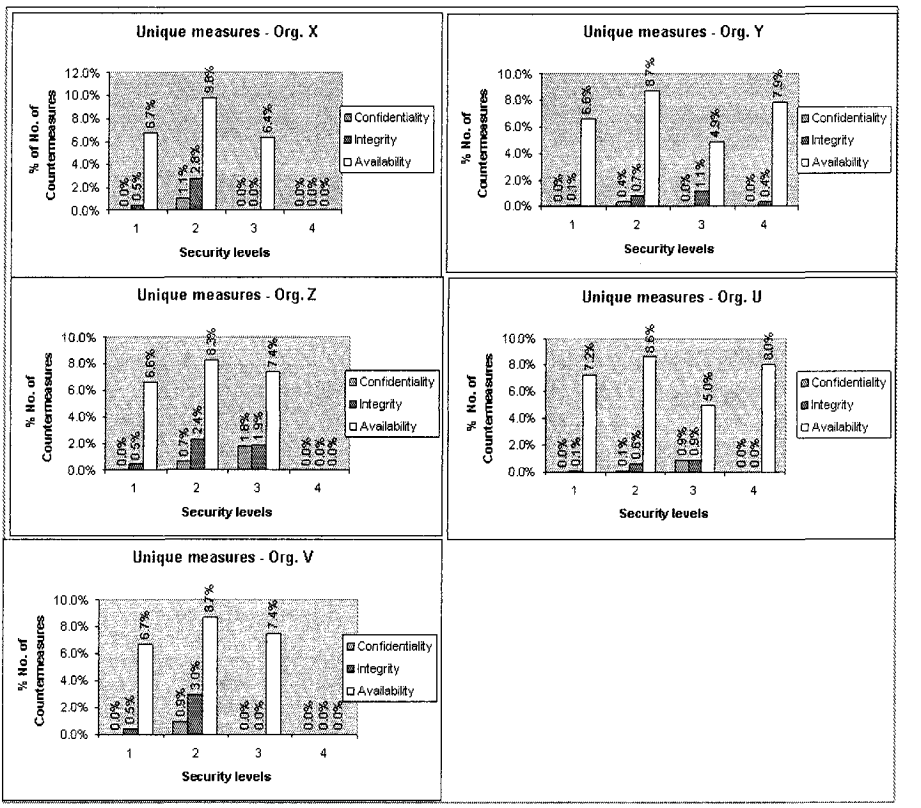

Figure 5. Percentage No. of Unique countermeasures vs. Security levels- Org. (X,Y, Z, U, V)

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

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

Example box 1

Information

Security Level 1

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

Property protected: Availability

5.1.2 Dual measures

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

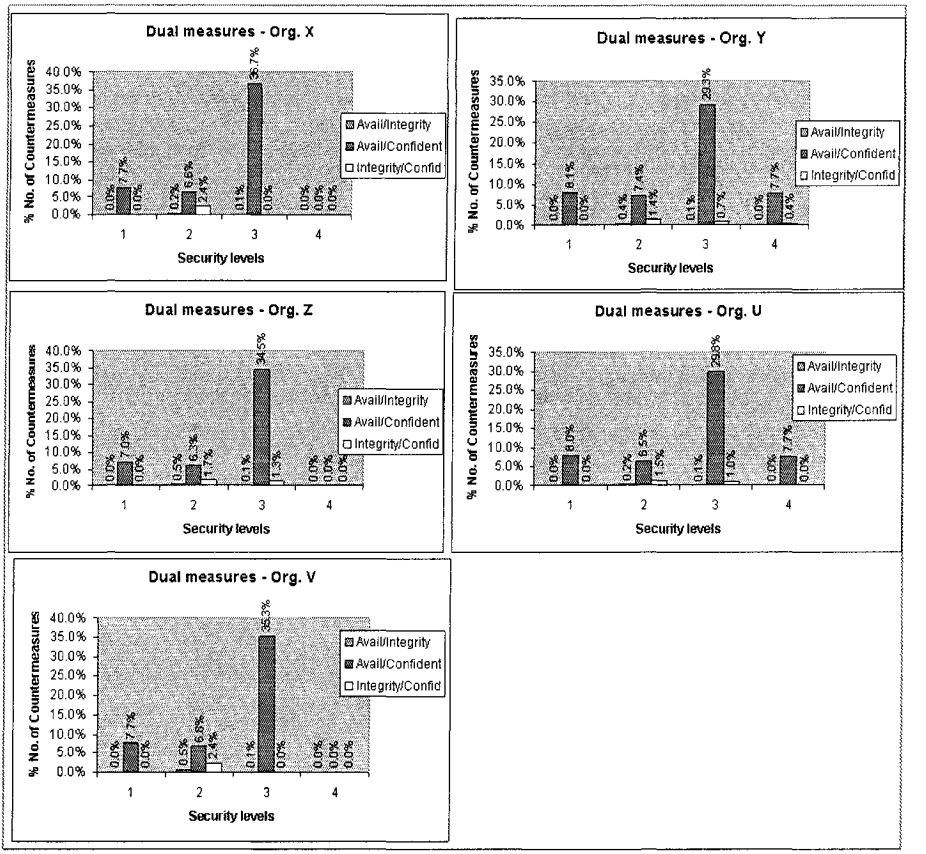

Figure 6. Percentage No. of Dual countermeasures vs security levels – Org. (X, Y, U, V, Z)

Example box 2:

Motorised pedestrian gates

Security Level 1

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

Property protected: Confidentiality, Availability

Security Level 2

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

Property protected: Confidentiality, Availability

5.1.3 Generic measures

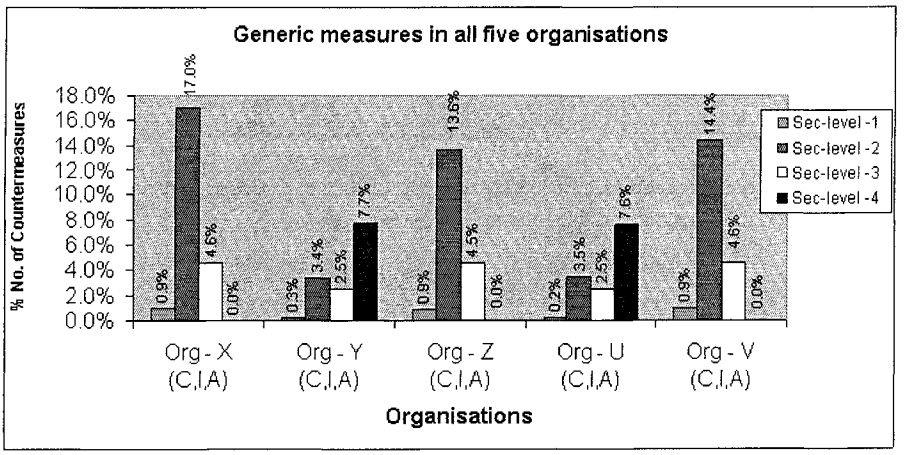

Figure 7. Percentage No. of Countermeasures vs. security levels – Org. (X, Y, Z, U, V)

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

Example box 3:

Organisation and Procedures

Roles and Responsibilities

Security Level 2

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

Property protected: Confidentiality, Integrity, Availability

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

5.2 Discussion

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

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

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

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

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

6. CONCLUSION

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

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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