Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)

Michael Kimwele mikekimwele@yahoo.com
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
P. O. BOX 62000- 00200 Nairobi, Kenya

Waweru Mwangi waweru_mwangi@icsit.jkuat.ac.ke
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
P. O. BOX 62000- 00200 Nairobi, Kenya

Stephen Kimani skimani@icsit.jkuat.ac.ke
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
P. O. BOX 62000- 00200 Nairobi, Kenya

Abstract

To address challenges faced by SMEs especially in Kenya, this paper aims to establish an Information Technology (IT) framework that can allow Kenyan Small and Medium Enterprises (SMEs) implement cost effective security measures. Particularly this paper discusses IT security requirements and appropriate metrics. There is evidence from the survey to suggest that despite having some IT security measures in place, Kenyan SMEs still face some serious IT security challenges. In the light of the challenges faced by Kenyan SMEs, this work recommends a framework which is supposed among other things provide some metrics of evaluating the effectiveness of implemented security measures. The framework is likely to assist SME stakeholders measure the effectiveness of their security enhancing mechanisms.

Keywords: Information Technology, Security, Metrics, Framework, Kenya, SMEs.

1. INTRODUCTION

IT security is often treated solely as a technology issue, when it should also be treated as a governance issue. In looking at the growing abundance of rules, regulations, and guidelines, it is clear that information security is not solely a technical issue, but also a corporate governance challenge.

Implementation of an effective IT security program is a matter of enlightened organizational interest. Companies are taking action to protect their own information and information entrusted to them by customers, suppliers, and other partners. They are establishing responsibility for information security in their companies and adopting programs to evaluate and address the vulnerabilities and the internal and external threats to their electronic information [1]

There is a lack of framework for action within SMEs- how to set priorities, assign tasks, get started and monitor implementation of IT security measures. To aid organizations in attacking the problem, numerous guides have been developed. These documents range from detailed technical guidance to high-level principles. But there is no recognized, standard approach at an organization-wide level to help in determining what should be done and who should do it [1]. Without such an approach, firms and particularly SMEs are unclear on how to allocate information security tasks, where to fund, and how to measure the return on investment [2].

We propose a framework that spells out what needs to be done by SMEs owners through borrowing lessons from other policy reports, guidelines, and combining these with our Kenyan experience through a survey (collected data) that was conducted to establish the current measures Kenyan SMEs have in place. This framework is supposed among other things to:

- Specify roles of SME owners in reference to IT security
- Indicate or spell out some metrics to measure the effectiveness of IT security enhancing mechanisms in SMEs
- Provide guidelines on implementation of IT security for SMEs in Kenya

The objective of the framework is to provide a way of tackling IT security challenges faced by Kenyan SMEs. In addressing this issue, this paper is organized into six sections. Following a brief introduction, the next section highlights some IT security requirements and metrics. Section three addresses the research methodology. Section four presents results and analysis. Section five discusses the recommended framework. The last section draws conclusions and future research directions.

2. IT SECURITY REQUIREMENTS AND METRICS

A survey of published literature shows that most reports on IT security [3], [4], [5], [6] cite the following requirements:

- The need for risk assessments. Risks must be understood and acknowledged and the IT security measures that are taken must be commensurate with these risks.
- The need for an IT security organizational culture.
- The need to create, communicate, implement, endorse, monitor, and enforce security policies across an organization.
- The need to make every member of the organization aware of the importance of IT security and to train them in good IT security practices.
- The need for access controls to make certain only identified and authorized users with a legitimate need access information and system resources.
- The need to monitor, audit, and review IT security measures regularly.
- The need for business continuity plans that are tested regularly.

We propose a framework that considers the above requirements in defining a coherent way of dealing with IT security in SMEs. In an endeavor to address IT security challenges in SMEs, there is need to resolve the following:

- Who is responsible for ensuring security?
- Who authorizes decisions that have to be made in regard to IT security?
- Who has to be consulted to ensure that every aspect of IT security is covered?
- Who has to be kept informed to ensure that the organization copes with resulting changes resulting from putting in place IT security measures?

To be able to measure the effectiveness of IT security measures in SMEs, our recommended framework requires that there should be some “IT security metrics”. IT security metrics are quantifiable measurements or any identifiable attributes that collectively characterize changes in security awareness/behavior of employees. It is against those metrics that the effectiveness of the proposed IT security measures in place can be evaluated.

IT security metrics should be designed to yield quantifiable information [7], [8]. The quantifiable information is useful for the following purposes:

- Comparison of security maturity
- Cost justification when insecurities occur can be clearly shown in metrics
- Indication and determination of critical and non-critical security parameters
- Redirect assets and set proper priorities for most critical security needs
- Security problem isolation

- Determine the effectiveness of security testing efforts

IT security metrics can be created to guide each aspect of security program including systems evaluation, internal security processes such as training and systems testing and risk assessment. The use of IT security metrics will allow organizations to determine effectiveness of implemented IT security processes, and control by relating results of IT security activities measurements [9].

IT security metrics may vary from one organization to another depending on the business environment of the organization in question among other factors [10]. Some of the IT security metrics which this research views are applicable to SMEs include but not limited to the following:

- Number of reported security incidents
- Number of viruses or other malicious code outbreak
- Number of comments on the IT security measures in place
- Number of reported cases for use of pirated software
- Traffic to unethical websites
- Number of virus problems resulting from opening unexpected email attachments
- Number of malicious codes resulting from downloading contents from untrusted websites
- Adherence to back up routines and procedures
- Frequency IT equipment failure
- Reported cases of compliance to IT security standards

It is by use of the above metrics that our framework finds their application in Kenyan SME environment with a view of using them to evaluate the effectiveness of implemented security controls. IT security metrics should be reviewed on a regular basis. During the review, new metrics should be developed and those found obsolete discarded. Each organization should develop its own set of IT security metrics.

3. RESEARCH METHODOLOGY

The different categories of primary data collection methods include laboratory measurements, field observations, archives/collections, questionnaires and interviews [11]. However, only questionnaires and interviews are suitable for the data required, as the opinions of a large and diverse group of people are needed. Questionnaires provide a more structured way of gathering and recording data. The research entailed a survey of SMEs in Kenya, were primary data was collected by means of a questionnaire. Most of the questions were adopted from previous studies but modified to capture data relevant to the current SME study. These were measured on a five-point likert scale whereby 1 represented “strongly agree” and 5 “strongly disagree”. A preliminary version of the questionnaire was discussed with scholars and managers. Some questions were reworded and the original structure of the questionnaire was amended.

This research is based on collected data which is then analyzed and organized to unveil some problems regarding IT security in Kenyan SMEs. We believe that to be able to address IT security issues effectively in SMEs, it is important to properly understand how IT security is currently being practiced in Kenyan SMEs. SMEs targeted in the survey included those in the consulting, recruitment, vehicle sellers, cleaning, legal, estate agent, medical, equipment leasing/rental, equipment repairs, and any others so long as the organization has got not more than 100 full time employees.

The sample consisted of:

- Formally registered businesses, the informal sector was not considered.
- The telephone directory was used to get regional distribution of SMEs
- Sectoral distribution of SMEs was based on national data from the Central Bureau of Statistics

The researchers administered the questionnaire over a period of four months between October 2009 and January 2010 to SMEs selected from all over Kenya. One hundred and twelve (112) SMEs were randomly identified to participate in the survey. The researchers then contacted the

SMEs requesting them to participate in the survey. Those who responded positively were then e-mailed the questionnaire which they were free to fill and e-mail back or they could fill and inform the researchers when to pick. In some cases, the questionnaire was delivered physically by the researchers and picked. The respondents were assured that all personal respondents would remain strictly confidential. Finally, twenty one (21) completed questionnaires were collected.

The respondents included business decision makers, IT managers, or people who take care of computers systems in SMEs. Out of the 21 SMEs that participated in the questionnaire survey, thirteen agreed to post-survey interviews to obtain “richer” information about IT security issues affecting them. As a consequence, in addition to responses to the questionnaire, other useful insights were also gathered. The exact of respondents in terms of nature of business, length of time the business has been in operation, current number of employees, number of computers used in the businesses and how long they have used computers are represented in Table 1 through to Table 5.

TABLE 1: What is the nature of your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Consulting	5	23.8	23.8	23.8
	Computers	3	14.3	14.3	38.1
	Equipment Repairs	2	9.5	9.5	47.6
	Other Professional Service	6	28.6	28.6	76.2
	Recruitment	1	4.8	4.8	81.0
	Vehicle Services	1	4.8	4.8	85.7
	Estate Agent	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

Table 1 shows the nature of the surveyed firms in terms of their operations. Majority of the enterprises are in Consulting and Professional Services.

TABLE 2: How long has the business in operation?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	9.5	9.5	9.5
	2	2	9.5	9.5	19.0
	3	1	4.8	4.8	23.8
	4	2	9.5	9.5	33.3
	5	3	14.3	14.3	47.6
	6	1	4.8	4.8	52.4
	7	2	9.5	9.5	61.9
	8	2	9.5	9.5	71.4
	10	2	9.5	9.5	81.0
	12	1	4.8	4.8	85.7
	14	1	4.8	4.8	90.5
	37	1	4.8	4.8	95.2
	89	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

Table 2 shows the length of time (years) the surveyed SMEs have been in operation. More than 90% of firms surveyed were less than 14 years old.

TABLE 3: What is your current number of employees?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-5	4	19.0	19.0	19.0
	11-25	6	28.6	28.6	47.6
	36-50	1	4.8	4.8	52.4
	51-	5	23.8	23.8	76.2
	6-10	5	23.8	23.8	100.0
	Total	21	100.0	100.0	

From Table 3, we note that majority of the SMEs surveyed had 11-25 employees (28.6%), followed by 6-10 employees (23.8%) and 51-upwards (23.8%).

TABLE 4: How many computers do you use in your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	9.5	9.5	9.5
	2	1	4.8	4.8	14.3
	3	2	9.5	9.5	23.8
	5	2	9.5	9.5	33.3
	6	1	4.8	4.8	38.1
	7	1	4.8	4.8	42.9
	9	2	9.5	9.5	52.4
	11	1	4.8	4.8	57.1
	14	2	9.5	9.5	66.7
	15	1	4.8	4.8	71.4
	25	1	4.8	4.8	76.2
	35	1	4.8	4.8	81.0
	40	1	4.8	4.8	85.7
	50	1	4.8	4.8	90.5
	60	1	4.8	4.8	95.2
	80	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

From Table 4, it is evident that more than 50% of the surveyed SMEs were using not more than 15 computers in their operations.

TABLE 5: How long have you been using computers in your

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	19.0	19.0	19.0
	3	2	9.5	9.5	28.6
	4	3	14.3	14.3	42.9
	5	2	9.5	9.5	52.4
	7	3	14.3	14.3	66.7
	8	1	4.8	4.8	71.4
	10	3	14.3	14.3	85.7
	14	1	4.8	4.8	90.5
	15	1	4.8	4.8	95.2
	19	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

19% of the respondents have been using computers in their operations for one year or less while 4.8% have been using computers for 19 years as shown in Table 5.

4. RESULTS AND ANALYSIS

The survey was conducted to establish the nature of IT infrastructure particularly its organization, employees and state of security measures. Through the interviews we conducted, SMEs pointed out the need for the following to be incorporated in a security enhancing mechanism for SMEs

- Create more awareness programs amongst SMEs and offer them related products to help in protection
- Education on the topic of Internet security
- Hold vulnerability seminars to try and show SMEs what goes wrong in their day to day operations

Considering the proportion and scope of SMEs in Kenya, poor information technology security of SMEs can yield catastrophic results both socially and economically. Among the issues considered in the survey, the following were found to be SME problem areas:

- Security Policy: 47.6% of respondents strongly agreed and agreed that their organizations have a well documented information security policy.

TABLE 6: We have a documented Information Security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	9	42.9	42.9	47.6
	Undecided	2	9.5	9.5	57.1
	Disagree	6	28.6	28.6	85.7
	Strongly Disagree	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

- Organizational Security: 38.1% of respondents reported having a director (or equivalent) member of staff being responsible for IT security.

TABLE 7: A Director (or equivalent) member of our staff has the responsibility for Information Technology security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	19.0	19.0	19.0
	Agree	4	19.0	19.0	38.1
	Undecided	9	42.9	42.9	81.0
	Disagree	3	14.3	14.3	95.2
	Strongly Disagree	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

- Personnel Security: Only 42.9% of employees have been trained to secure their computers at all times, especially when moving away from their workstations.

TABLE 8: Staff have been trained to secure their computers at all times, when moving away from their work stations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	19.0	19.0	19.0
	Agree	5	23.8	23.8	42.9
	Undecided	3	14.3	14.3	57.1
	Disagree	7	33.3	33.3	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

- Communications and Operations Management: 47.6% of respondents reported that they are confident, that in the event of equipment failure, theft or a site disaster, their back ups and storage would enable them to retrieve their information systems with minimal business interruption.

TABLE 9: We are confident, that in the event of equipment failure, theft or a site disaster, our data back ups and storage would enable us retrieve our information with minimal business interruption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	14.3	14.3	14.3
	Agree	7	33.3	33.3	47.6
	Undecided	3	14.3	14.3	61.9
	Disagree	6	28.6	28.6	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

- Business Continuity Management: 28.6% have a business continuity plan which specifies who must take action and what has to be done to ensure that the organization can continue functioning in the event of a disaster such as a fire/flood.

TABLE 10: We have a business continuity plan which specifies who must take what action and what has to be done to ensure that the organization can continue functioning in the event of a disaster such as fire/flood

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	5	23.8	23.8	28.6
	Undecided	7	33.3	33.3	61.9
	Disagree	6	28.6	28.6	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

- IT Security Standards: Despite the fact that there are some standards which organizations can adopt, 52.4% of SMEs surveyed reported that they were aware of any standards they could adopt.

TABLE 11: Prior to this survey, I was aware that there are established, international information security standards, available for organizations to adopt

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	14.3	14.3	14.3
	Agree	8	38.1	38.1	52.4
	Undecided	2	9.5	9.5	61.9
	Disagree	6	28.6	28.6	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

In view of the above problem areas, we recommend that SMEs should adopt the following in their quest to realize enhanced IT security:

- Development of IT security policies
- Identification of roles and responsibilities of each individual regarding IT security
- Make all employees aware of IT security issues
- Select and implement appropriate security measures
- Put in place data recovery measures in case of accidents
- Identify and protect all organizational assets that need to be protected
- Adopt appropriate IT security standards

We aim at synthesizing from the discussions, analysis, and interpretations made so far in an attempt to establish a means that can help in evaluation, formation, and implementation of possible IT security controls to address the security situation observed and described in the previous section. Based on empirical analysis of security practices in organizations, this work proposes a framework that can be used to evaluate SME IT security measures.

The resulting framework brings together numerous concepts into a coherent explanation that should be useful for SMEs or any other individual seeking to evaluate the effectiveness of implemented security measures. Because of limited IT budgets for SMEs, the framework is necessary to enable SMEs evaluate IT security measures at low costs.

5. IT SECURITY FRAMEWORK FOR SMES

Our recommended framework consists of the following:

- A mapping of identified IT security metrics and the IT security issues/activities/aspects the metrics can measure (Table 12).
- An approach for tackling IT security issues which deals with continual improvement and establishment of new measures should the implemented ones at any one particular time appear ineffective (Figure 2).
- An illustration of how the approach can be utilized in an IT security enhancing mechanism for SMEs. This illustration is done using data that was collected during the survey (Table 13).

		IT SECURITY METRICS									
		Number of reported security incidents	Number of viruses or other malicious code outbreak	Number of comments on the IT security measures in place	Number of cases for use of pirated software	Traffic to unethical websites	Number of virus problems resulting from opening unexpected email attachments	Number of malicious codes resulting from downloading contents from untrusted websites	Adherence to back up routines and procedures	Frequency of IT equipment failure	Reported cases of compliance to IT security standards
IT CONTROL ISSUES/ACTIVITIES/ASPECTS	**Security Policy** (Is our IT security policy effective?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Organizational security (Is there a Director or equivalent member of staff responsible for IT security?)			✓						✓	✓
	Asset Control (Can all assets including hardware and software used for information security handling be identified and located?)								✓		
	Personnel Security (Are Staff aware that security incidents should be reported to management immediately?)	✓	✓	✓							
	Physical and Environmental Security (Is there appropriate physical and environmental security procedures in place to prevent interference with business premises and IT systems?)			✓						✓	
	Communications and Operations Management (Are we confident that our anti-virus systems are up to date, and in the event of a virus outbreak, we should be able to protect our systems?)	✓	✓				✓	✓			✓
	Access Control (Can users logon/gain access to our systems without being formally registered with their own user account?)			✓							✓
	System Development and Maintenance (Can our systems provide audit trails so that usage of the system and data input/changes can be audited?)		✓			✓		✓			✓
	Business Continuity Management (Have our security measures been reviewed within the last year?)								✓		✓
	Compliance (Is our organization aware that there are established, international IT security standards available for adoption?)	✓									✓

TABLE 12: Mapping of IT Security Metrics and the IT Security Issues/Activities/Aspects they can Measure

Table 12 demonstrates various IT security control issues/activities/aspects and the metrics which can be used to measure such issues. Although metrics have been proposed over a long period of time, an ideal metrics is one which is easy to understand, effective and efficient [12]. In order to develop an ideal metric, metrics should be validated and characterized effectively.

For a security awareness program to be effective, it has to be recursive and must be evaluated on regular intervals based on predefined corporate awareness metrics [10]. Casmir [10] further suggests that an organization's information security program should be recursive and cyclic in nature as depicted below:

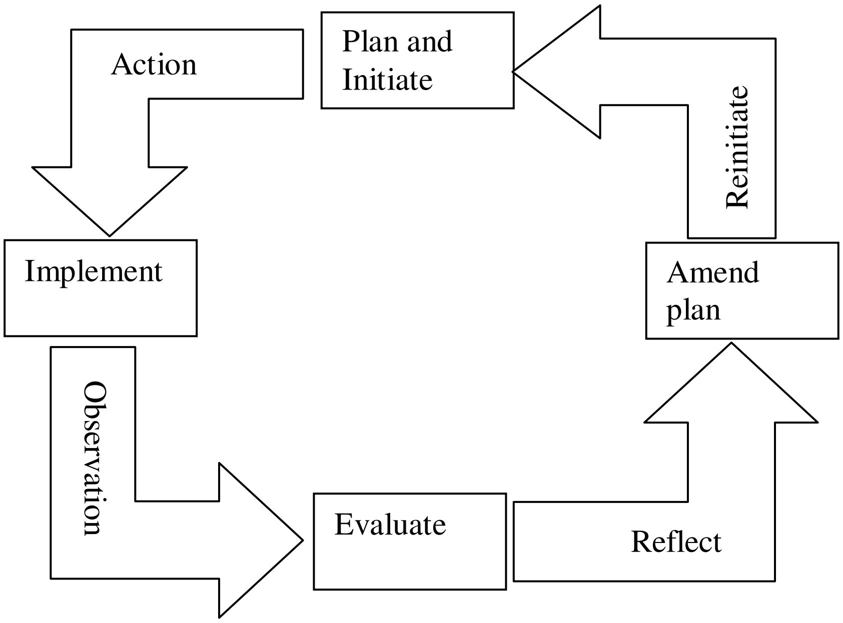

FIGURE 1: Information security awareness program lifecycle [10]

Our framework recommends the following approach to tackling IT security issues in SMEs (Figure 2). This approach is based on the recursive lifecycle put forward by Casmir (Figure 1).

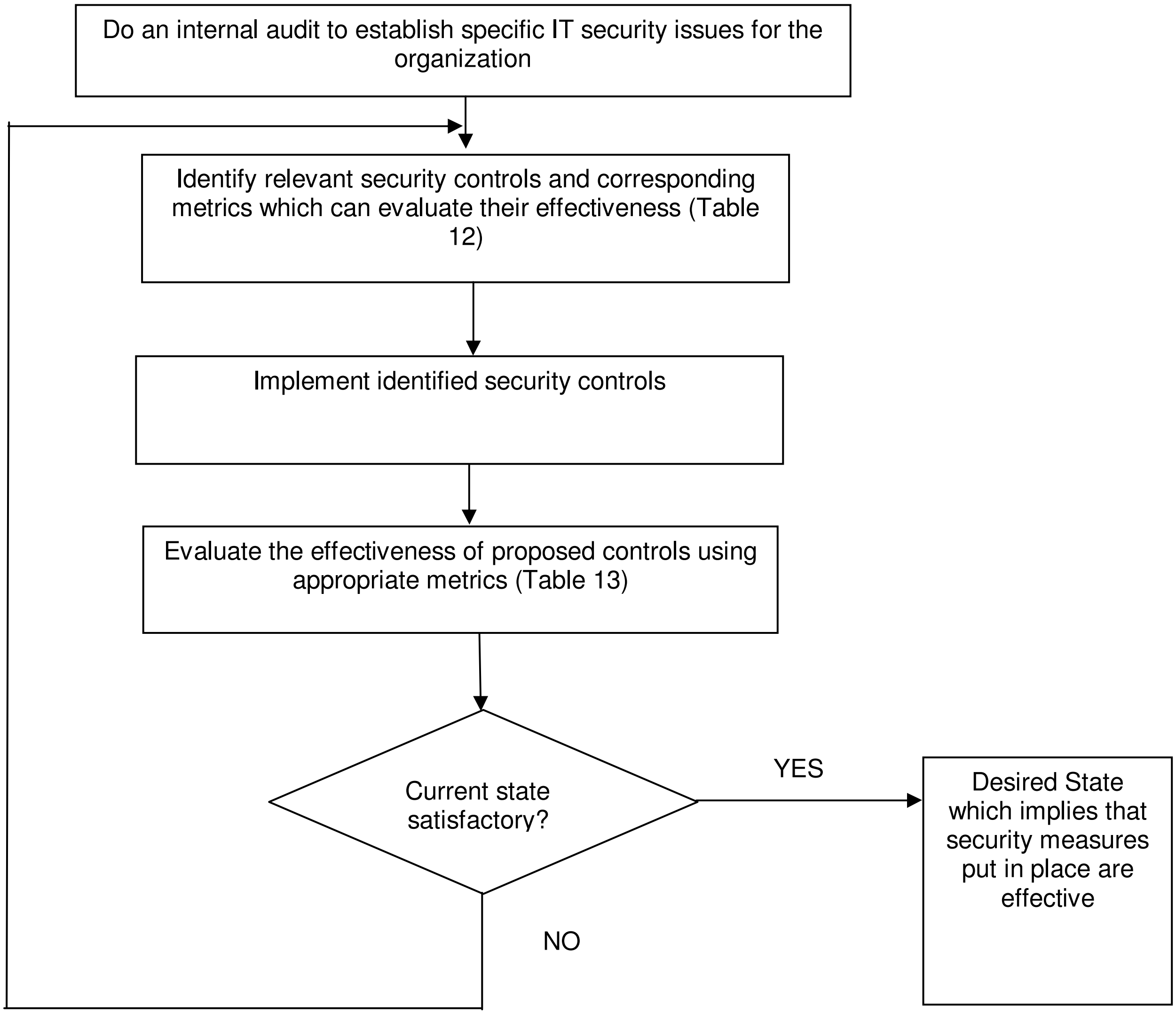
Do an internal audit to establish specific IT security issues for the organization
Identify relevant security controls and corresponding metrics which can evaluate their effectiveness (Table 12)
Implement identified security controls
Evaluate the effectiveness of proposed controls using appropriate metrics (Table 13)
Current state satisfactory?
YES
Desired State which implies that security measures put in place are effective
NO

FIGURE 2: Approach for evaluating the effectiveness of IT security measures in SMEs

In Table 13 below we provide a summary of selected SMEs in terms of the security controls they have in place and then evaluate them in light of the security breaches the organizations have suffered within the past year. Through this it is possible to examine and show that some measures are effective than other based on experience of the surveyed SMEs.

IMPLEMENTED SECURITY CONTROLS	**SME 1**	**SME 2**	**SME 3**	**SME 4**
Have a security policy	YES	YES	YES	YES
A director (or equivalent) member of staff has responsibility for IT security	NO	YES	YES	YES
All assets can be identified	NO	YES	YES	YES
Security incidents are reported to management immediately	NO	NO	YES	YES
Have appropriate physical and environmental procedures	YES	YES	YES	YES
Up to date antivirus systems	YES	YES	YES	YES
Proper system access control mechanisms like user accounts	YES	YES	YES	YES
System usage audit trails	NO	NO	NO	NO
Security measures have been reviewed within past year	YES	NO	YES	YES
Adopted/Complied with IT security standards	NO	NO	NO	NO
SECURITY BREACHES SUFFERED WITHIN PAST YEAR				
No information security breeches				
Inadvertent breech (e.g. user accidentally deleted files or changed computer configuration)	✓	✓		
Deliberate attack (e.g. hacker/disgruntled staff gained access, deleting or stealing data)			✓	✓
Asset theft (e.g. software application misplaced causing re-installation delay/costs)	✓	✓		
Equipment failure (e.g. hard drive crashed causing loss of data and business disruption)	✓		✓	✓
Back up failure (e.g. system restore failure due to corrupt/ inadequate back ups)			✓	
Data theft (e.g. espionage which resulted in data loss and possible legal exposure)				
Site disaster (e.g. fire or flood causing damage to systems and business disruption)	✓			
Copyright infringement (e.g. staff loading pirated software, legally exposing the organization)	✓			✓
Compliance (e.g. passing on confidential information, legally exposing the organization)	✓			

TABLE 13: Implemented Security Controls and Security breaches suffered within the last year

The above checklist (Table 13) is an illustration of the use of the recommended approach in Figure 2 above. The illustration is based on four randomly selected SMEs from the survey. It shows that despite SMEs having implemented various security controls, they still suffered various security breaches within the past one year. This is essential in determining whether the current state of affairs (security controls in place and resulting reduction/increase in security breaches) is satisfactory. In the event that the security breaches increase in number and the organization considers them significant, then as per our approach, new controls should be established and the process as shown in figure 2 iterated/repeated. This process should continue until the organization is satisfied that the security measures/controls in place yield the desired results/state in terms of IT security.

It is worth appreciating the fact that in our checklist (Table 13) time is essential since the security breaches have to be observed and reported over a determined time (say, one year). This helps in measuring the effectiveness of implemented security controls and is also consistent with the way other metrics are established/defined. For instance, Reliability can be defined as the ability of the software product to perform its required functions under stated conditions for a specified period of time, or a specified number of operations. Reliability can be measured using 'mean time between failure' (MTBF), which is the average time between successive failures [12]. A similar measure to MTBF is 'mean time to repair' (MTTR) which is the average time taken to repair the software after a failure occurs.

6. CONCLUSION & FUTURE WORK

To address current difficulties of organizations reluctant to invest in IT security due to cost, this work proposes an IT security implementation framework that will allow SMEs adopt cost effective security measures whose effectiveness can be evaluated using appropriate metrics.

This framework is significant in that it allows SMEs to take necessary security measures and to realize what actions they can take in case they are faced with IT security issues. This will help SMEs protect their information assets. It is also significant in that it is a new approach presenting an IT security framework for SMEs that is recursive and cyclic and therefore can be improved continually in line with the changing IT security landscape.

Since the framework has not been tested in a real working environment of SMEs, further analysis on the effectiveness of the framework is required, and the results should be reflected in future frameworks.

ACKNOWLEDGEMENT

The authors would like to thank the German Academic Exchange Service (DAAD) for funding this research.

7. REFERENCES

1. B. Conner et al., (2004), Business Software Alliance, http://www.bsa.org [20/8/2010]

2. R. Casmir and L. Yngstrom (2005), Towards a Dynamic and Adaptive Information Awareness Approach. In proceedings of the fourth world conference on information security education, Moscow, Russia, ISBN: 5-7262-0565-0

3. C. T. Upfold and D. A. Sewry (2005), An Investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape.

4. C. N. Tarimo (2006), ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach, Stockholm University, Department of Computer and Systems Sciences, December 2006.

5. M. R. Pattinson and G. Anderson, G (2007), "How Well are Information Risks being Communicated to your Computer end-users?" Information Management and Computer Security, Vol. 15. No. 5. (2007), pp 362-371

6. R. Werlinger et al. (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security", Information Management and Computer Security, Vol. 17. No. 1. (2009)

7. M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo (2003), Security Metrics Guide for Information Technology Systems. http://csrc.nist.gov/csspab/june13-15/sec-metrics.html [16/8/2010]

8. P. E. Ammann P. E and Black, P. E. (2001), "A Specification-Based Coverage Metric to Evaluate Test Sets", International Journal of Reliability, Quality, and Safety Engineering, Vol. 8 No. 4, pp 275-300; Singapore, World Scientific Publishing.

9. J. A. Chaula (2006), "A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance", Stockholm University: Department of Computer and Systems Sciences, Report Series/DSV No. 06-016, ISSN 1101-8526

10. R. Casmir (2005), A Dynamic and Adaptive Information Security Awareness (DAISA) Approach, Stockholm University, Department of Computer and Systems Sciences, December 2005.

11. J. A. Sharp and K. Howard (1998), The Management of a Student Research Project, 2nd Edition. http://www.hlss.mmu.ac.uk/infocomms/people/staffpub/rjh.doc [12/2/2010]

12. R. Khurana (2007), Software Engineering: Principles and Practices, ITL Education Solutions Ltd, New Delhi, India, 2007.