International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:6, No:10, 2012

Information System Security Effectiveness Attributes: A Tanzanian Company Case Study

Nerey H. Mvungi, Mosses Makoko

***Abstract*—**In today's highly globalised and competitive world access to information plays key role in having an upper hand between business rivals. Hence, proper protection of such crucial resource is core to any modern business. Implementing a successful information security system is basically centered around three pillars; technical solution involving both software and hardware, information security controls to translate the policies and procedure in the system and the people to implement. This paper shows that a lot needs to be done for countries adapting information technology to process, store and distribute information to secure adequately such core resource.

***Keywords*—**security, information systems, controls, technology, practices.

I. Introduction

INFORMATION systems security in enterprises which includes organizations, government departments or its organs is of primary concern since they use information technology (IT) in their core business processes. Confidentiality, integrity, and availability of information must be assured at all times by deploying appropriate security technologies. However, security has to be enforced by policies and practices and enhanced by controls making reliability of information systems to be a function of technology, processes and people [1-2]. This paper evaluates these three pillars of IT security to find out their effectiveness and the role played by each component.

Executives in developing countries have excelled in physical security of information involving guards, CCTVs, lock and key since information was stored in physical form. The soft storage of information in the IT era needed a different approach. Enterprises in developing countries chose technological solutions to protect their information assets without clear protection strategies and change of mindset. However, where they were strategies no efforts were made to ensure that employees appreciated them being the enforcers. Hence, a gap was created between the enterprise's operational practices and the set of security controls making employees to misconceive controls as a stumbling block.

A significant number of senior officers in an enterprise command chain did not appreciate or gave high priority to IT security and control measures needed to enforce the IT security policies through IT security controls. This can be attributed to hangover of the security administrative controls meant for information stored in physical media. Most staffs are not normally fully aware of the enterprise's mission or business-related needs, hence its relation to controls in the IT systems for their enterprise. However, they participate in the design and in enforcing security controls. Their appreciation of various control needs is crucial for them to effectively use fully the security features offered by the security technology used.

Significant enterprise administrators perceive that perfect protection of information resource can be achieved through technology based security controls alone. Hence, it is significant to change this perception and to classify types of information assets and the means of protection. This is because different information resources have different degree of sensitivity and may be subjected to different levels of risk. Therefore, it is important that measures are taken to ensure that controls, practices and technology in the ICT policy are observed and revisited to reflect the dynamic nature of ICT and its usage. It is essential to ensure seamless communication between business units of the enterprises and the IT departments to minimize security risks to an acceptable level. Therefore, the effectiveness of information security technologies, practices of people that use information systems and controls in place in preventing unauthorized access, disclosure and disruptions to enterprises' protected information resources has to be assessed.

II. Information Security

Security of information requires protection of data from unauthorized access, use, disclosure, destruction, modification, or disruption. In addition, it concerns authenticity, accountability, non-repudiation and reliability of the protected information [3]. The credibility and image of the enterprise is influenced by the reliability of its information based on the ability to guarantee its confidentiality, integrity and availability. The main thrust being cultivating user's trust and confidence. Security processes in an enterprise are meant to realize this irrespective of accidental or intentional action of user, system or intruder from internal or external [4]. Security technologies like encryption, backups, redundancy, authentication, authorization, safeguards, etc. aims to address threats and vulnerabilities.

A. Enterprise Information Systems Security

Enterprise information is a valuable asset; hence it has always been well protected to safe guard its integrity,

N.H. Mvungi is with the College of Information and Communication Technologies, University of Dar es Salaam, P.O. Box 35194, Dar es Salaam, Tanzania. (phone: +255-22-2410556; e-mail: nhmvungi@ udsm.ac.tz).

M. Makoko is with Vodacom Tanzania Ltd, P. O. Box 2369, Dar es Salaam, Tanzania. (phone: +255-754-710473 e-mail: mmakoko@vodacom.co.tz).

confidentiality and availability to ensure business continuity, minimize business risk and maximize return on investments and business opportunities to achieve organizational goals and mission [5]. The increased global interconnection and competition has been a catalyst for increased sophistication in threats and vulnerability to information resource.

The complexity of large enterprises and the desire to automate processes to create competitive advantages; increases dependence on technology hence making security a challenging task. Therefore, security must be embedded in organizational and operational context considering it as a business problem that the enterprise must activate, coordinate, deploy and direct in its core competencies functions [6-7]. Security management processes has to be technical, strategic, systematic and repeatable.

It is necessary to classify information to be protected and protection efforts are directed appropriately to include the roles of users, owners and custodians in the classification schemes [8].

B. Security Technologies

Information security technology is multi-disciplinary effort to avail systems that increases resilience from intentional attacks, errors or mistakes focusing on the tools, processes and methods while being adaptive to environment and business requirements changes [9]. The list of deployed technologies is very long so for brevity it is omitted here.

C. Security Practices

Practices are the techniques and methodologies used by people to implement policies, principles, procedures, rules and processes to protect information systems. Hence, to implement IT security successfully mindset change is important. The owner has to mould the mindset of employees at all levels and ensure that they follow set security policies, rules and procedures. Proper practices calls for diligence involving the level of judgment, care and prudence [10]. Furthermore, proper practices call for segregation of duties in IT systems operations. It is common to find an individual being the systems administrator and information security Director hence taking total control of the IT system subjecting it to individual's actions vulnerability.

Each process involved in the implementation of security objectives must have an owner. To achieve effective information security governance, best practices requires that controls be defined by operational managers and implemented by IT staff within a defined control framework for all information systems security processes [10].

D. Controls

The problem is controlling subjects (persons or programs) access to objects (files, programs, databases, internal hardware resources, input and output devices). Controls are facilitated by technical solutions and operationalised by different players in the system. Table I shows typical key players. Controls manage policies, risks and practices and enforce procedures and guidelines or organizational structures. There are three basic controls categories: preventive, detective and corrective.

In addition there are deterrent and applications controls. There are several also application controls like input, output and processing controls. The controls can be implemented using administrative techniques (people practices), technical means (technology itself) and physical devices (securing access).

Accountability is another means of control that require subjects to provide identity and authentication information which includes non-repudiation. Controls are often defined by the job or role an employee plays in an enterprise.

TABLE I
COMMON ROLES AND RESPONSIBILITY

Role	Description
Senior manager	Has the ultimate responsibility for security
InfoSec officer	Has the functional responsibility for security
Owner	Determines the data classification
Custodian	Preserves the information's C.I.A.
User/operator	Performs in accordance with (IAW) the stated policies
Auditor	Examines security

III. STUDY TEST BED

A telephone company in Tanzania offering wide ranging telephone and IT services was used as a case study on effectiveness of controls, technology and practices in providing security to its information resource but wishes to remain unanimous for commercial reasons. The majority of the Company's Network is digital, which includes transmission and switching systems. They have in place synchronous digital hierarchy (SDH) systems enabling IP network used for Next Generation Network (NGN) to carry Call Data Records (CDRs) of fixed network, Broadband information and Code Division Multiple Access (CDMA) Traffic. The network is exposed to the Internet at some gateway points, which poses a security risk. The company's internal network is comprised of a Wide Area Network (WAN) covering all regions and almost all districts in the country. The information security officers from IT department are responsible for security of employees' information and security of company's internal operations.

The company had distributed information security control initiatives from the network department to information technology department. This study focused on IT department where there was formal security function done by three security officers.

The study used informal, unstructured, formal, structured and interactions interviews. In addition, security initiatives documents were consulted. In some cases technical tests were performed to check validity of information provided by respondents.

Questionnaire to test technical and controls awareness and practices for providing IT security was also utilized for the three targeted group namely technical, executives and ordinary staff. The group was further refined to 9 groups to include competence level in IT.

A. Technology

Technology here refers to the deployed infrastructure and applications to provide effective security controls. Technologies were used to test effectiveness of the controls directly, monitor compliance with enterprise policies and account for and analyze security incidents. In addition, they were used to assist in reassessing identified risks and appropriateness of existing controls and identifying new controls and risks [11].

For the study case firm, its network was complex which was a WAN VPN and its applications complex requiring high level of security because of the sensitivity of the data handled. The system required a layered, defence-in-depth security strategy. This study was centred on access, system integrity, cryptography, audit and monitoring and configuration management and assurance controls.

The file server being central repository for all user files was chosen to study the effectiveness of access control technology and security of data. A number of security factors were observed like hardening and optimization of operating system and the relisation of company's information security policy.

B. Practices

Practice is the weakest link in any security infrastructure since secure use of information systems depends largely on the practices of its users [12]. For example, using inappropriate password will circumvent an otherwise secure system. Training on security awareness and rewarding those following procedures is an effective tool to build a security-conscious environment where everyone understands its importance and their role. Practices are governed by process that involves policies, procedures and rules. Poor practices may result in lawsuits, lost revenue, bad publicity and basic security attacks. In this study, best practices considered only five categories; access controls management, computer and network management, personnel security management, business continuity management and information security management.

C. Controls

Controls is the employment of means and devices to promote, direct, restrain, govern, and check upon its various activities for the purpose of seeing that objectives are met. Hence, security controls are management, operational, and technical measures prescribed which, taken together, satisfy the specified security requirements and protect the confidentiality, integrity, and availability of the system and its information. Only five factors were considered in this study: Components used to establish control, types of controls, control characteristics, control standards, and control implementation.

IV. Qualitative Observations

A. Security of Application Programs Inadequate

A number of application programs and critical databases had weaknesses that increased the risk of access by unauthorized user to critical business information were lacking.

Observation 1: Configurations were not reviewed periodically, configurations enabled authorized users to perform unauthorized activities, little or no documentation of current configuration settings, and process unable to accurately identify, monitor and report on IT assets.

Observation 2: The adherence to controls standards was very strong. Only systems meeting the SDLC standards were allowed to operate in the IT system. However, documentation was poor not showing even changes to an application program tests, independent review and approval. The mediation fixes for the billing system was the most affected but yet central to the very existence of the company.

Observation 3: There are strong procedures set to control system software changes. However, the controls were circumvented in some systems such as payroll. There were no procedures to test changes in program codes making it difficult to detect such changes. Therefore, security features could be inadvertently or deliberately omitted or "turned off" or the risk of processing irregularities or malicious code introduced.

B. Inappropriate Network Security

The several network security weaknesses identified were:

- User IDs and passwords could be captured from an internal network using social engineering techniques and/or freely available hacking software.
- Active network connections were in conference rooms, and all around workplaces.
- Network user ID and password management was not effective and passwords allowed and used easily guessed.
- Retired or resigned employees had active network IDs.
- Many active network IDs had never been used.
- In the server, important files were left with default settings hence accessible to all. System Administrator could do anything to such files.

C. Physical Controls not Adequate

The company did not have approved procedures for granting and periodically reviewing access to computer and telecom resources. It was observed that there was inadequate prevention of physical access control to network equipment and power room, radio and transmission sections, and that anyone having access to the building could access wiring closets.

D. Business Continuity Management Lacking

- A business continuity plan (BCP) had not been developed for the company.
- A disaster recovery plan was in place, but after the review only one disaster recovery plan (DRP) for a payroll system was developed, but not implemented.

E. No formal Information Security Awareness Program

There was IT Policy but no security policy. Execution of security activities had the following shortcomings:

- Lack of coordination between IT security sections and other operation sections dependent on IT services.
- Documentation of security processes very poor.

- Employees and/or contractors upon cessation of employment or contract not removed from the system.
- There was no regular follow-up of remote access users to establish need for such facility.
- There were no regular verification of users' access privileges in relation to their roles and responsibilities.
- There was no process for regular update of the latest security patches/fixes.

F. Personnel Bad Practices Rampant

Several unacceptable practices in the profession of information security were observed. They included:

- Using first or last names as passwords and sharing them.
- Confidential information stored on laptops because its risk was unknown or lack of trust of the file server.
- Downloaded freely from untrusted internet sources.
- Rarely used Microsoft office password facility to protect word and excel files.
- There were no procedures for disposing sensitive electronic documents while shredders were in all offices for disposing of sensitive paper documents.
- Good security practices and safeguarding confidential information was perceived as IT personnel problem.
- Confidential information in plain text was attached to emails while staff had no confidentiality agreement with employer.

G. Unfavorable Security Control Environment

The executive management understanding of information security issues was either limited hence was not given the required attention which provided non-conducive IT security environment. The following were observed in regard to controls:

- Information systems audit reports showed consistently the risk assessment was outstanding, but no action was.
- There were in place many types of controls implemented except for the automated detective control of intrusion detection/prevention system and use of biometrics.
- Placement of controls management was wrong and competence was inadequate. This was attributed to the control policy design itself. An example, a control for software change management is placed in finance department under the financial systems control manager having no competences in IT.
- There were no security software and hardware to facilitate monitoring security violation logging, and reporting.

H. Poor Information Security Management Practices

Several unacceptable practices in the management of information security were observed. They included:

- Senior management displayed little commitment to information security initiatives.
- There was no information classification.
- There was no accountability since system ownership and custodianship practices were lacking.
- New technologies were implemented without proper information security planning.
- Confidentiality agreements were lacking.
- Security processes were driven by technology rather than corporate business processes hence integration between them was inadequate.
- No alignment between information security and company's objectives; emphasis was on technical issues.
- Executive and line management ownership and accountability controls implementation lacked.

V. The Survey

Survey made focused on factors that contributed significantly to security concerns. The survey instruments (questions) were designed using the information obtained from qualitative observations made to qualify them. IT security awareness of the company stakeholders was included in the survey being a principal attribute to the practices IT security factor. The questionnaire had both closed and open types of questions. The main categories of stake holders involved in the survey with or without IT background were normal users, technical and management staff, and the company executives (heads of units and chief executives).

A. The Survey Sample and Response

The participants with exception of virtual of office (the executives) were randomly selected to avoid biasing the outcome. The return rate of questionnaires shown in table II was highest for the groups with IT background. Follow up of those who did not respond showed that it was an attitude problem towards IT. Normal users did not see it as their problem while executives gave time availability excuse.

TABLE II
QUESTIONNAIRE DISTRIBUTION TO STAFF AND RESPONSE

Group	Category	Questionnaires		
		Distributed	Collected	
Normal Users	Normal Staff	24	63%	64%
	Managers (Without IT Background)	15	67%	
Technical Staff	IT Staff	10	90%	95%
	Data Engineers	5	100%	
	Managers (With IT Background)	4	100%	
Executive Management	Heads (With IT Background)	2	100%	58%
	Heads (Without IT Background)	4	50%	
	Chief Executives	6	50%	
Total		70	71%	

B. Survey Results

The survey results were analysed using the Statistical Package for Social Scientists (SPSS). There were seventeen basic questions asked in the survey; selected sample of the responses are provided in this section.

The response to a question seeking perception of employees on use of password enabled by technology to provide information security to the company is shown in fig. 1 while that of greatest challenge in realizing strategic information security policy is that in fig. 2. The response on drivers that influenced employees information security practices awareness of information security function in their company is given by fig. 3.

Tests on whether they considered themselves playing part in enhancing security when new security features are introduced is given in fig. 4. Fig. 5 shows results for the kinds of technologies adopted to secure information and the assessment of appropriateness of the selected one is provided by fig. 6.

C. Follow up Observations Based on Survey Results

There was ineffective maintenance of security application programs since there were no configuration management systems and important system documents. This made recovery operations after incident cumbersome.

- There are some of the executives who were overriding controls on change management on soft ware systems.
- Network security weaknesses can be attributed to weak security policies and procedures that did not address well all stakeholders. System administrators were able to randomly take ownership of user files to read, modify or even delete without leaving audit trail.
- Risk assessment to identify critical assets was not there.
- There was no implemented and fully tested disaster recovery plans for all systems other than payroll.
- There was no security awareness programme.
- Poor personnel behaviour on information security was attributed to inadequate security control environment since there was no information governance framework or information security governance. Information security problems needed to be elevated in governance levels.

VI. Reflection from Observations

The effectiveness of security controls in information systems was observed to be limited mainly due to poor practices rather than the technology used. There is strong interdependency between these three factors in realizing effective information system security although controls are central but is facilitated by appropriate technology that can be compromised by poor practices.

A. Technology

- Appropriate choice of technology is fundamental to minimize hacking success chances. This need be guided by clear understanding of what is to be protected.
- Inappropriate utilization of acquired protection system features was evident. Mostly default settings were used.
- Traceability of actions of actors in the IT system was compromised.

B. Practices

- Best practices may make even a rudimentary security system more effective than a sophisticated one where all norms are floated. Hence, behaviour of employees is critical in security enforcement. Technology and control schemes provide facilitation.
- It is misconceived that providing security is the responsibility technical team/management.
- Technology as a strategic security driver of corporate culture is not customer-centric, entrepreneurial or having commercial acumen hence not embraced in management practices other than IT personnel.
- Corporate culture rather than accepted industry's best information security practices dominated personnel behaviour.
- Management practices not taking up information security control corporate culture when introduced.
- Long time employee embraced security corporate culture not necessarily in line with best information security practices. They concentrated on control concepts applicable to physical storage media.

C. Controls

- Complex system was in place but controls were unintentionally overlooked/overridden due to limited knowledge and experience of the system or self interest.
- Highly complex operations result in fatigue of systems and people. For example systems access rights were given randomly during change over to meet deadlines and the problem was never corrected later.
- Knowledgeable IT staff worked to determine unique methods to circumvent controls.
- Some employees had negative attitude towards controls and continuously attempted to damage, defeat, or ignore them. This was also used to sabotage management when its relationship with employees was not good.
- Employees treated controls indifferently intentionally considering it as bureaucracy or hindrance to their personal gains or unintentionally in a form of misunderstanding. Hence, it is a very big challenge to enforcers of controls in such a situation requiring the enforcer to be very strong and to understand very well IT security control systems.
- Intentional falsifications of volume of data or customer base size or reconciliation to either portray control systems as ineffective or higher efficiency than reality.
- Intentional misinterpretation of results from intentional erroneous entries to the actor's advantage.
- Dissatisfied staff undermined the success of controls by making mistakes and being carelessness. They took leave while in critical system migration or went home at end of working hours even when the system was down.
- Misuse of executives' controls override card to enable other non-deserving employees to ignore controls.
- Perceived controls as an impediment to achieve their goals.
- Inadequate systematic mindset change of staff on controls.

VII. Conclusion

Correct hardware and software are necessary but not sufficient criteria to ensure effective information security in an enterprise. Related operational weaknesses like change management, segregation of duties, security awareness and audit, access management, etc must be understood and addressed. Furthermore, comprehensive enterprise IT security management program must be in place and implemented.

It is also necessary to have correct people with correct attitude in place in order to achieve the desired information security.

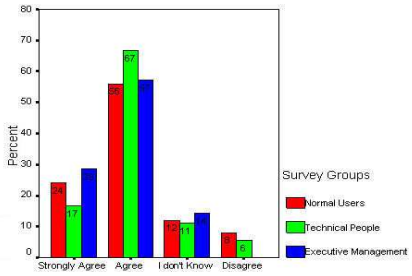

Fig. 1 Perception of use of password (technology) to enhance information security

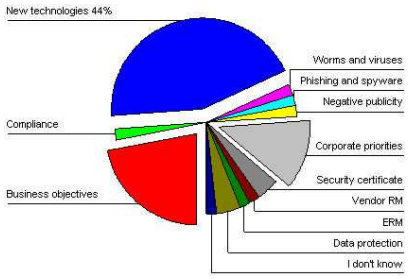

Fig. 2 Factors influencing employs behavior
Vendor RM = Vendor Risk Management ERM = Enterprise Risk Management

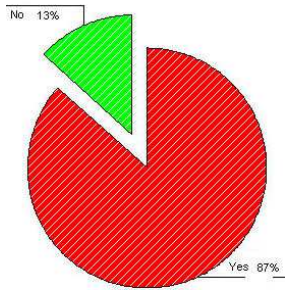

Fig. 3 Employs awareness of IT security function

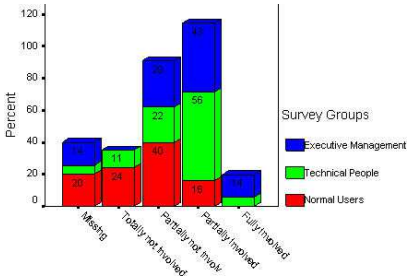

Fig. 4 Perception of involvement in new security

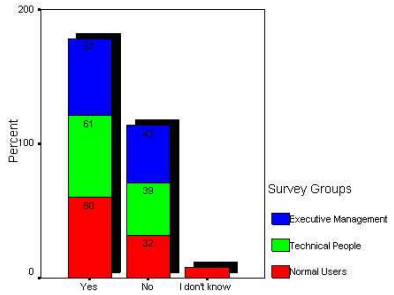

Fig. 5 Security enhancement features technologies

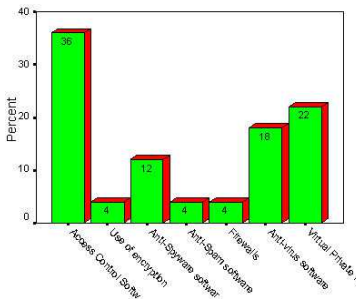

Fig. 6 Appropriateness of selected technology

The enterprise used as case study in this work had state of the art security systems but wrong practices in implementing security controls made controls to be compromised at all levels. The technical personnel capitalized on the ignorance/ carelessness of their executives or collusion to override crucial business related security controls. Mindset change on IT security concepts to adapt to soft storage of information resource in networked world was inadequate.

The study has clearly demonstrated that a very sound and sophisticated information security technical solution can be rendered useless if it is not embedded in company's corporate culture, appropriately integrated in management process and having appropriate policies that are properly and adequately owned. The challenge to technocrats is can we contain this?

REFERENCES

[1] C. Alberts, and A. Dorofee, "Managing Information Security Risks: The OCTAVE Approach", 1st Edition, USA, Addison Wesley, 2002.
[2] A. Andress, "Surviving Security: How to Integrate People, Process, and Technology", 2nd Edition, New York, USA, Auerbach Publishers Inc., 2004.
[3] F. Gallegos, "Educating the Masses: Audit, Control and Security of Information Systems Today and Tomorrow" Information Systems Control Journal, 2004 Vol.6, pp13-15.
[4] Kurtz, R.L. and Vines D.V., "The CISSP Prep Guide - Mastering the Ten Domains of Computer Security", 1st Edition, USA, John Wiley & Sons Inc, 2001.
[5] Ward, J. and Peppard, J., "Strategic Planning for Information Systems", 3rd Edition, West Sussex England, John Wiley & Sons Inc, 2002.
[6] Doughty, K., "Implementing Enterprise Security: A Case Study (Part 1)", Information Systems Control Journal, 2003 Vol.2, pp34-39.
[7] Doughty, K., "Implementing Enterprise Security: A Case Study (Part 2)" Information Systems Control Journal, 2003 Vol.3, pp60-63.
[8] Federal Financial Institutions Examination Council (FFIEC), "IT Examination Handbook: Information Security", USA, FFIEC Publishers, 2006.
[9] Ross, S. J., "Information Security and the Resilient Enterprise", Information Systems Control Journal, 2005 Vol.2, pp8-9.
[10] O'Bryan, S. K., "Critical Elements of Information Security Program Success" Information Systems Control Journal, 2006 Vol.3.
[11] W. Stallings, "Cryptography and Network Security Principles and Practices", 4th Edition, USA, Prentice Hall, 2005.
[12] H.F. Tipton and M. Krause, "Information Security Management Handbook", 5th Edition, New York, USA, Auerbach Publishers Inc., 2003.