Evaluation of Data Security Measures in a Network Environment Towards Developing Cooperate Data Security Guidelines

Ayub Hussein Shirandula
Dr. G. Wanyembi
Mr. Maina karume
Masinde Muliro University of Science and Technology

***Abstract*— Data security in a networked environment is a topic that has become significant in organizations. As companies and organizations rely more on technology to run their businesses, connecting system to each other in different departments for efficiency data security is the concern for administrators. This research assessed the data security measures put in place at Mumias Sugar Company and the effort it was using to protect its data. The researcher also highlighted major security issues that were significantly impacting the operations of Mumias Sugar Company. The researcher used the case study methods where both qualitative and quantitative data was collected by use of questionnaire, interviewing and observation. From the findings the researcher developed data security guidelines for Mumias Sugar Company. The information gained from extensive literature review was tested and observed during the case study.The research revealed that data security lapses in the company was as a result of system administrators' failure to update and train computer users in the company on how to implement different data security measures that were in place. The final outcome of the research was data security guidelines that were practical enough to be used at Mumias Sugar Company.**

Keywords- Data, security; security measures; guidelines; computer users; Mumias Sugar Company.

I. Introduction

Today, most companies need information systems to prosper and survive for too long. Data has now become a valuable asset to modern organizations. Therefore it was imperative for Mumias Sugar Company to take the protection of their information resources seriously. (Geer, 2003), Lack of knowledge in the organization is the greatest threats to data security (Mitnick & Simon 2002). Without adequate level of user Corporation and knowledge, many security techniques are liable to be misused or misinterpreted by users which may result in an adequate security measures becoming inadequate (Sponen, 2001).

Most people believe that it is impossible to set up a computer system in a network environment and ensure that the system is secured. According to (Connolly, 2000), "the only secure system is one that is completely disconnected from a network and lying off the bottom of the ocean" it is a fact that "data security is an information technology hot issue as long as a computer is networked" (Connolly, 2000)

A. General Objective

The general objective of this research was to establish how the companies' data security could be determined by the data security measures that it had put in place and how it required different controls. In order to improve the data security of MSC, it was important to review data security measures that the company had put in place.

B. Specific Objectives

Main objectives of this research were:

1) *To asses and analyze the security measures being used in the company.*

2) *To evaluate the security measures being used in the company with existing security standards such as ISO 17799.*

3) *To develop cooperate data security guidelines for the company on how they can use different security measures to ensure the adequacy of its data security.*

C. Research questions

The following research questions were selected to address the stated problems.

1) *Which data security measures does Mumias Sugar Company have in place?*

2) *How is Mumias Sugar Company using the different data security measures it has set up?*

3) *How can Mumias Sugar Company develop data security guidelines to use different security measures it has established?*

D. Purpose of the Study

For Mumias Sugar Company to accomplish its strategy it had heavily invested in computerization, several of its departments were computerized. This research was essential for the networked environment of the company. The challenges of computerization had adversely affected the farmers and the management, where they had complained over the distortion of data in the company. Some farmers had supplied canes without payments, a fact that leads to slow the advancement of Mumias

Sugar Company. The researcher was assessing the security measures that were being used at the company.

This research contributes literature on how Mumias Sugar Company data is assured of its confidentiality, integrity and availability. A comprehensive framework was developed for Mumias Sugar Company to be able to safeguard its data and information resources from theft, abuse, misuse and any form of damage. Responsibility and accountability of information was assured at the end of the research.

E. Conceptual frame work

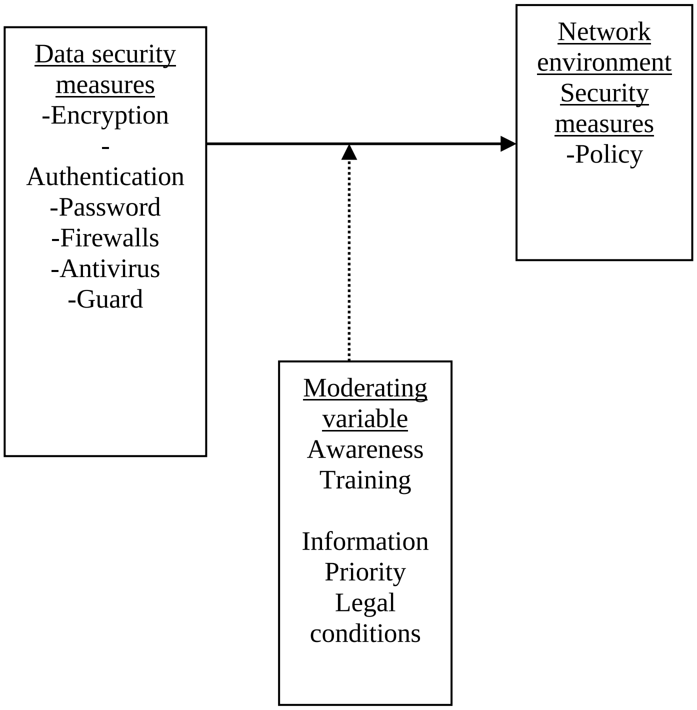


Figure 1. data security measures and its moderating variables

In the network environment existing data security measures were available. This data source was developed independently and was divided into three parts (Figure 1). Considering the complexity of securing data in a networked environment of MSC, the researcher proposed a newly designed data security measures system which was particularly designed to address the needs of the Mumias Sugar Company. By extracting the data from the original data sources the researcher improved and simplified the data security measures structure, address awareness, training, information priority and legal conditions which was important for data encryption, authentication, password, firewalls antivirus and guard (Figure 1). The conceptual framework manages the loading and updating of the data security measures.

F. Literature review

Large number of organization focuses on the technical defenses such as, encryption, access control, firewalls and intrusion detection that is associated with information protection (Ande,1972 & sand, 1996) however there was little comprehensive research that focused on how companies should: prepare for facing security incidents by selecting appropriate security measures, evaluate their present vulnerability (risk) to security incidents, asses the damages of past security incidents, train security personnel in law enforcement agencies to better prepare for dealing with security incidents.

The major problem associated with information security is that the damage is invisible and its existence is unknown. This causes difficulties for managers to justify their investments on security. (Butl, 2002 & Cohe, 1991).

The most serious financial losses in organization are related to theft of proprietary information. Information is a key resource in global competition. Organizations spent a reported 15% of the IT 2006 budget on information security and increased the rate of security staff hiring, but did not realize improvements in enterprise security, according to 2006 annual security survey (Berinato,2007).

From the literature new threats to information systems occur from unexpected sources when organizations become more reliant on it (Nyanchama, 2005). “Threat is an indication of impending danger or harm” (Johnson, 2008). “A security threat is a condition of vulnerability that may lead to an information security being compromised.” (Kumar, Park, and Subramaniam, 2008).

In 2008 95% of crimes in the sphere of information were personal data thefts with 93% in 2007. Today practically everyone admits that the only way to provide information security is to take a complex approach combining measures at four levels: legislative, administrative, procedural, programmed-technical and economic.

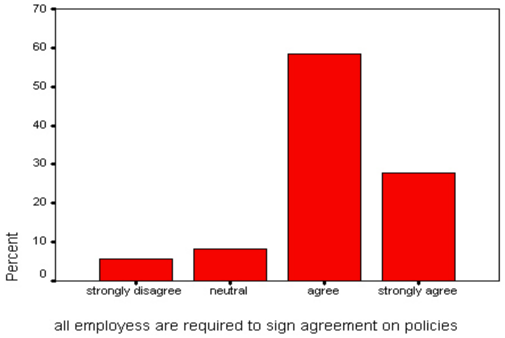
G. Qualitative and Quantitative Research Methods

Studies require different methods depending on the purpose and type of the research. Various literatures have extensively discussed the many different approaches of gathering data but most distinction is made between qualitative and quantitative methods. The aim of qualitative research methods was to explore reality through an investigation of human aspects such as feelings and behavior. In this study human behavior was observed.

While the quantitative approach explored numerical and quantifiable aspects as per (Maylor & Blackmon, 2005). In order to draw general conclusion of this research we needed measurable data (quantitative approach). But in order to increase understanding of security issues in the company in depth we needed to use qualitative approach to answer “why” and “how” questions as per (Johnson, 2004). For this research, the facts clearly suggested that we used the two approaches.

H. Views on Security Policy

1) Majority of the employees (90%) confirmed presence of a formal Policy in their company. Regarding update all information security policies were reviewed at least once a year and updated as needed. 86% of those who were interviewed confirmed that all employees were required to sign an agreement verifying they had read and understood the security policies and procedures (Refer to Graph.1)



Graph –1 All employees are required to sign agreement on policies

2) A periodic revision of the Policy brings many benefits for the company. When asked how often they revised their Policy? 73.3% interviewed replied once annually basis. However, they should be doing it on as needed basis.

3) In case of any security incident in the company response plan was formally documented and disseminated to the appropriate responsible parties. All security incidents were reported to the person responsible for security investigation. There was an incident response team ready to be deployed in case of any a data compromise.

I. Opinion regarding the implementation of control measures.

All users are required to authenticate using, at a minimum, a unique username and password which is changed after every three month. 50% strongly agreed that they change their password, however they reported that they were not trained on how to generate those passwords hence they faced problems of forgetting from time to time. (See table 1)

TABLE I. ALL USERS ARE REQUIRED TO AUTHENTICATE USING PASSWORD

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	***neutral***	3	8.3	8.3	8.3
	agree	15	41.7	41.7	50.0
	strongly agree	18	50.0	50.0	100.0
	Total	36	100.0	100.0	

All passwords on network devices and systems were supposed to be encrypted. From the literature review it has been observed that password used mostly is not. When asked whether all passwords used is encrypted? On the scale of 1-5, with 5 being ‘strongly agree’, 23% employees choose ‘5’, where as 24% choose scale ‘4’

J. Findings and Conclusion:

Data security largely depends on combinations of different security measures. Security policies and awareness plays a very key role among other measures. Through this research several data security measures were investigated. Finding suggest that implementing proper security measures is getting more crucial especial in a networked environment. Further findings and conclusions are discussed below.

1) A formal physical restriction to data was found to be present in more than 70% of the company’s departments. This imply that the companies management was giving due importance to data security. However there were some lapse i.e. from the findings it shows that the company did not have the right procedure on how to handle secure distribution and disposal of back up.

2) Finding suggested that more than 90 % of the departments used authentication (user name and password). The users believed use of unique username and password was final to securing data. All computers on the network had password which was not encrypted. From the findings it shows that when an employee moves from one department to the other 70% of the accounts and password remained intact. 72% of those interviewed disclosed that user accounts were not reviewed on a regular basis to remove unknown ones. All accounts that were inactive were not automatically disabled in the system after a predefined period.

3) Virus protection as a data security measures: all computers in the company were loaded with antivirus software. 77 % of staff contacted, were a ware of some of the signs that could indicate computer had contracted a virus. The finding shows that more than 60% of the staff was not aware of what they could do if they suspect that there computer had a virus. More than 60 % of staff contacted reported that there storage devices, software or data that originated from outside were not scanned or checked for virus prior being used. From the findings it showed that the work of updating and ensuring that the computer was up to date was left for the IT security officer. Formalization of all information security policies, including policies for access control, application and system development, operational, network and physical security formally were not documented in more than 80% of the departments. Awareness and training program was not part of company Security policy.

K. Guidelines for Mumias Sugar Company Security Rule Compliance

The research presented above leads to a discussion of data security and security measures that are appropriate for the MSC. Data security measures refer to different data security mechanisms based upon the companies view of its data, values of the data and users of the data. Value of the data is determined by the company. Data to be secure requires various types of control measures. The common problem across the board is the ownership of the data and its privacy. The various control measures all relates to companies management. This part includes development of guidelines which form the framework to support this research. Various security measures that have been explored is mainly because of the value the companies data has. Administrator builds data protection; ICT technical staff maintains service levels and companies systems because of the company’s data. Maximizing data security at MSC requires company involvement for which we present the following set of guidelines

L. *Recommended practices*

The following list identifies all the practices that should be implemented. Considerations for Technical Solutions, provides discussion regarding selected technical solutions.

- Account Management
- Information Management
- Disaster Recovery
- Electronic Mail
- Data Centers
- Remote Access
- Information for Users
- Workforce Identity
- Continuity Planning

M. *Workforce Identity and Account Management*

1) Determine which individuals are authorized to work with the network computer in the company in accordance with a role-based access approach.[164.308.a.3] [A]

2) Establish data security and control measures training for all members of the company workforce who are involved in the creation, transmission, and storage of the company's data. Ensure that training program includes periodic security reminders and is updated to take into account current vulnerabilities and threats. [164.308.a.5][a]

3) Take disciplinary action in accordance with MSC personnel policies and guidelines on workforce members who fail to comply with MSC policy and procedures, including information security policy and procedures.

4) Ensure the verification of the individual or employee who is authorized to access MSC system and that the person is correctly bound to a unique user identification ("sign-in") for access to the system [164.308.a.4][A] [164.312.a.1][R]

5) Ensure appropriate access controls mechanisms for authorized users' access to any MSC system. For systems with the very sensitive data, require strong electronic authentication, such as sufficiently complex passwords or use of other encryption key mechanisms to access the companies systems containing data. [164.308.a.5][A].

6) Establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals or entities who have terminated or no longer are authorized to access MSC systems [164.308.a.4][A].

7) Carefully manage system administrator accounts to ensure the accounts are used for only specific system administration functions. The number of these accounts should be kept to a minimum and provided only to personnel authorized to perform identified functions. Passwords or other authentication measures should be changed upon the termination of systems personnel who accessed these accounts.

8) Log activities performed by system administrator accounts and monitor logs on a regular basis.

Reference

[1] Butler, S. A.(2002) "Security Attribute Evaluation Method: A Cost-Benefit Approach,"

[2] Geer, D., Soo Hoo, K., J., Jaquith, A.(2003) "Information Security: Why the Future Belongs to Quants," IEEE Security and Privacy.

[3] Mitnick, K., & Simon, W.(2002) The art of deception: Controlling the human element of security. Wiley Publishing.

[4] Siponen, M.(2001) Five dimensions of information security awareness. Computers and Society, June 2001, 24-29.

[5] Anderson J. (1972) "Computer Security Technology Planning Study," U.S. Air Force Electronic Systems Division Tech. Rep.

[6] Cohe F(1991)., "A Cost Analysis of Typical Computer Viruses and Defenses,"Computers & Security.

[7] Sandhu, R. S.(1996) Coyne, E., J., Youman, C. E., 1996, "Role-based Administration of Rules," ACM Transactions of Information Systems.

[8] Berinato, S. (2007). The end of innocence. CIO Magazine. Retrieved, from http://www.cio.com/article/133600/

[9] Johnson (2008). Information risk of inadvertent disclosure: Journal of Management Information Systems.

[10] Kumar & Park (2008). Understanding the value of countermeasures portfolios in information systems security

[11] Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management.