Vol II Issue X

ISSN No : 2230-7850

Monthly Multidiciplinary Research Journal

Indian Streams Research Journal

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Indian Streams Research Journal
Volume 2, Issue.10,Nov. 2012
ISSN:-2230-7850
Available online at www.isrj.net
ORIGINAL ARTICLE

A STUDY ON PROBLEMS AND PROSPECTS OF INSTALLING COMPUTER SECURITY MEASURES IN SELECTED SUGAR FACTORIES

BABASAHEB JOTIRAM MOHITE

Assistant Professor,
Sinhgad Institute of Business Management (MCA), Kamalapur.
Tal. Sangola, Dist. Solapur

Abstract:

In today's rapidly changing scenario, individuals and organizations are relying heavily on automated computer systems to store, retrieve, process and exchange information. Organizations use's the information stored on these systems to conduct vital business operations. Therefore, organizations need to protect the information from unauthorized access and potential destruction. Earlier, an organization, computer system was developed, used and maintained in isolation from other areas of business. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. IT managers, Network Administrators and Database Administrators face increasing challenges of managing and protecting information and network resources from unauthorized access. So to preserve data securely every IT user must know the benefits and losses about the computer security. Which are the different threats to computer data and which are the different security controls and policies required to maintain data security?

In view of the above, the present research work "A Study on problems and prospects of installing computer security measures in selected Sugar factories" has come up for further in-depth study.

KEYWORDS:

Threats, Integrity, Virus, Password, Hacking, Biometrics, Fire extinguisher.

INTRODUCTION:

In this era of IT, every individual and organizations are highly relied on computer system to avail benefits of computer system characteristics like speed, accuracy, storage capacity, versatility and even security to their businesses. Organizations spend Lakhs of rupees and expend thousands of man-hours to maintain their information systems. Now days every organization is using computer systems for storing, accessing, processing and transmitting data in digital form at minimum cost, to generate different types of information which are very helpful for decision making and carry out day-to-day routine work smartly. It is therefore necessary that every IT user should be aware about different computer security risks, benefits and losses of maintaining computer security, threats to computer systems, as well as detective and preventive measures against different security threats. The user should be aware of the legal aspects and the policies required for maintaining the security of the available information.

2 STATEMENT OF THE RESEARCH PROBLEM

In view of the aforesaid discussion, the researcher would like to dugout different micro

perspective of these problems to suggest solution(s) on the enormity of such problem for efficient management of computer security mechanisms and processes. Thus, the present research work entitled “A Study on problems and prospects of installing computer security measures in selected Sugar Factories” has come up for further in-depth study.

3 OBJECTIVES OF THE STUDY

The present study is designed to focus on the above mentioned computer security issues with the objectives listed below.

1.To study and examine
-The computer security measures adopted by the selected Sugar organizations.
-Problems of installing computer security measures in Sugar organization and their causes

2.To suggest measures for efficient computer security and general security.

4 HYPOTHESIS OF THE STUDY

The study is also undertaken to test following hypothesis-

1.Organizations have no significant awareness of different security technologies in the vicinity.
2.Organizations are not having adequate mechanism for computer security maintenance.

5 SIGNIFICANCE OF THE STUDY

Like any other business system, computer system is also subjected to be victim of unwelcomed threats, arises intentionally or accidentally. Due to these different management members from Sugar organizations are in very much tense about maintaining privacy of their business data. Also the suppliers of sugarcane are only and totally rely on the computer security mechanism provided by sugar organizations for their valuable data. If any organization fails to maintain faith of their shareholders, may suffer huge financial loss, also may compel to face different legal problems such as IT act 2000 and Indian penal code Section 406, 420 etc. The study thus conducted will prove useful to the sugar factories under study operating in Sangli and Kolhapur district in particular and to other sugar units in general.

6 RESEARCH METHODOLOGY ADOPTED

Sample units: To serve the purpose of the research subject, the researcher has selected the total 12 sample units out of total 36 sugar factories from Sangli & Kolhapur district, whose daily crushing capacity is more than 3500 MT. These parameters were being used with a view to identify and find out the sample units who have huge administrative work and who have installed computer systems adequately and also have computerized varied functional areas of their business operations. Next, researcher has selected sample respondents from these sample units to obtain the necessary information. These sample respondents' are- One Management representative (Managing Director), One EDP department Head, and

Table No.1 : Breakup of sample respondents

District	Sugar Factories		
	Sample Units	Respondents per unit	Total respondents
Kolhapur	9	7	63
Sangli	3	7	21
Total	12	7	84

ımpling technique	:	Purposive Quota Sampling.
›pulation	:	Sugar factories from Sangli and Kolhapur district
ze of population	:	36 Sugar factories from Sangli and Kolhapur District
ıalysis units	:	A plants of Sugar factories

Size of sample : 84 respondents.
Parameter of interest : Determining problems and prospects in installing computer security measures in selected sugar and dairy organizations.

Data required: For the present research work, the data related to the following mentioned aspects was of prime importance:

·PROFILE OF SUGAR UNITS

· Status of existing computerization, applications and system software details, security awareness level of employees, available security mechanisms.
· Problems related to installing and monitoring computer system.
In order to achieve the objectives of research study and to obtain the aforesaid data, the researcher has categorized the data into primary and secondary data and resorted to primary as well as secondary sources of data collection.

DATA COLLECTION SOURCE:

a) Primary Data – The primary data was collected through fact finding techniques like personal interviews and discussion, on-site observation and administering structured questionnaire. The researcher has prepared three sets of questionnaire for Managing directors, Heads of EDP department and for computer operators.

Secondary Data – In order to avail the secondary data necessary for the study, researcher has personally visited related government and semi-government organizations, sugar factories websites and libraries.
Data Analysis: The data so collected through varied sources was analysed in a systematic way through tabulation, percentage and graphical presentation. Similarly the hypotheses set were too tested with the help of statistical tools like Chi-square test.

7 SCOPE OF THE STUDY:

- Geographical Scope: The geographical scope of the present study cover selected Sugar organizations in Sangli and Kolhapur District only. The sugar units studied on the magnitude of its problems and prospects pertaining to installing computer security measures.

Topical Scope: The topical scope of the present study is restricted to study various concepts regarding maintaining and installing computer security, identify current status about security measures adopted and awareness level of users in the selected Sugar units only.
Analytical Scope: This study covers all the aspect of the objectives preset for the study. The data collected and analyzed with the help of simple statistical tool (Percentage). This study also assists to test the hypothesis preset for the study with the help of statistical tools such as chi-square method etc.
Functional Scope: The functional scope is confined to offering a set of meaningful suggestions about maintaining computer security, about security policies and installing computer security measures.

8 VALIDITY OF THE STUDY:

Proposed research is aimed to focus on the current situation of computerization and data security measures adopted at different Sugar organizations under study.
-This research will reflect the present scenario of the awareness level of computer security to the concerned and will prove useful for better performance.

9 LIMITATIONS OF THE STUDY

a.Conclusion drawn from the survey is limited for Sugar units of Sangli and Kolhapur district only.
b.Secrecy was maintained by the respondents while interviewing and filling questionnaire in respect of some of the information, and hence some of the respondents could not discuss freely.

Hypothesis 1: Organizations have no significant awareness of different security technologies in the vicinity

Technology	Aware with technologies	
	Yes	No
Fiber optic cable	3	9
Firewall Security	12	0
Antivirus Software	12	0
Server based access control list	2	10
Intrusion Detection Systems	4	8
Intrusion Prevention Systems	4	8
Encryption of data for transit	0	12
Encryption of data on storage	10	2
Log Management Software's	2	10
Digital Certificates	2	10
Biometrics	12	0
Group Policies	0	12
VPN	0	12
Motion detectors	0	12
Fire alarm system	0	12
Smoke detection system	0	12
Fire extinguisher	12	0
Dynamic alarm system to notify changes	0	12
Security and Patch updates	9	3

Chi-Square calculation Table (Using Yates Correction Rolling technique)

Observed Values			Expected Values	
Yes	No	Total	Yes	No
3	9	12	8.2105	13.7895
26	10	36	24.6316	41.3684
4	8	12	8.2105	13.7895
4	8	12	8.2105	13.7895
10	14	24	16.4211	27.5789
4	20	24	16.4211	27.5789
12	60	72	49.2632	82.7368
12	12	24	16.4211	27.5789
9	3	12	8.2105	13.7895
85	143	228		

Chi-square value	1.87003E-20
P value	15.5073131
Degree of Freedom	8
Interpretation	NULL Hypothesis Accepted

Here, the calculated Chi-square value is less than the P value at 5 percent level of significance at 8 degree of freedom. Therefore we accept the Hypothesis and conclude that 'Organizations have no significant awareness of different security technologies in the vicinity.'

Hypothesis 2: Organizations are not having adequate mechanism for computer security maintenance.

Security mechanism	Having?	
	Yes	No
Fire alarm system	0	12
Smoke detection system	0	12
Fireproofing ceiling	3	9
Air conditioning	11	1
Motion detector	0	12
Separate arrangement of electricity & N/w cables	12	0
Fire extinguisher	12	0
Security guard	0	12
Maintain Entry & Exit records for visitors	0	12
Dynamic alarms to notify change to security configuration	0	12
Power contingency plan	0	12
Licensed software's	12	0
Login & Password	12	0
Static IP address	4	8

Chi-Square calculation Table (Using Yates Correction, Polling techniques)

Observed Values			Expected Values	
Yes	No	Total	Yes	No
3	33	36	25.9286	40.0714
11	13	24	17.2857	26.7143
24	48	72	51.8571	80.1429
28	8	36	25.9286	40.0714
66	102	168		

Chi-square value	1.97457E-18
P value	9.487729
Degree of Freedom	4
Interpretation	NULL Hypothesis Accepted

Here, tl ated Chi-square value is less than the P value at 5 percent level of significance at 4 degree of freedo fore we accept the Hypothesis and conclude that, Organizations are not having adequate mecha computer security maintenance.

10 FINDINGS

1.Units under study have not made provision of IT budget in their annual budget and also do not have a separate ISM department to handle computer security maintenance related issues. It is also found that not a single unit has a dedicated IT planning or steering committee to supervise the IT function and its activities.
2.Most of the organizations are having Windows XP Operating system on their computers.
3.Not a single member from any organization under study has completed any IT Security Maintenance Course.
4.All organizations are having UPS facility of power conditioning and surge protection to shield electronic equipments from power spikes. But still some organizations are not having adequate UPS facility when electricity fails.
5.All organizations under study are having Client- Server Network facility, and Majority of organization is using UTP cable for Network communication.
6.Majority of organization members have experienced Hardware fault, Virus, Human negligence and Environmental Hazard, but very few of them experienced Data alteration, Data destruction threat. Not a single Operator and Management representative experience threats like Hacking, Data alteration and Data destruction.
7.In most of the organizations, their server room and other areas of computer installation are having fire extinguishers, Separate arrangement for electricity and network cables, Air conditioning and fireproofing ceiling but not a single organization is having Fire alarm system with emergency power off system, Smoke detectors, humidity and dehumidification equipments, Motion detectors. Also no Security guards appointed at restricted areas like server room, backup room etc. Neither have they had Maintained entry and exit records for visitors and outsiders to departments, nor having Dynamic alarms to notify the changes to any security configuration from Insider or Outsider.
8.About 50 percent organizations individual computers used by more than one user, also 50 percent different person uses unique username and password on the system.
9.Not a single IT staff from any organization has signed a confidential agreement about data security.
10.No organization is using a system which have features like audit log generation, reporting and tracking feature for un-authored access attempts or manipulation of data. Also none of the organization has applications that encrypt data before Storing, Sending it over the Internet or an open network.
11.Near about 82 percent organizations are familiar with different National security Acts, but not a single organization is familiar with International security Act like SOX, GLBA, HIPAA etc.
12.Very few IT Heads attended data security conferences, trainings, refreshers and seminars, whereas not a single computer operator attended any data security conferences, trainings, refreshers and seminars. Not a single organization is having any formal disciplinary process for staff that violates data security policies and procedures. And also no any reward or appreciation system followed in these organizations for those who perform well on Information Security Management.
13.Not a Single organization has conducted formal risk management activity, and has appointed a data security officer nor IS Auditor.
14.Majority of organization perceive limited human resources, limited budget, and political influences as the top hurdle to good security measure in organization.

11 SUGGESTIONS

From the overall observation and findings it can be concluded that, to carryout proper and rigid security plans some suggestions on the basis of findings are –

1.All the selected organizations are having 100% network facility mainly carried out with the help of UTP cables with no other security measure than login user name and password to secure from the unauthorized access. Hence to increase data security level the organizations should –
-Use Fiber Optic cable instead of UTP or Co-axial cables, because the data communication speed and data transmission security is more as compare to UTP and Co-axial cables.
-Implement firewall to secure the network from outside world or unauthorized requests.
-Install Network intrusion detection systems like Network based IDS, Host based IDS or combined IDS.
-Use Server OS like Linux or Novell which are most secure from virus attack or difficult to hack for outsider intruder.

2.Suggestions for selecting, training and creating user of computer system are-
-Appoint an IT staff who has completed at least 1 years University or private degree course in computer and

also compulsory conduct the background check on selection of IT staff.
-Arrange or make compulsory to attained conferences, refreshers, trainings and seminars on essentials of computer security.
-Get signed on confidential agreement about data security.
-Create separate logins for each user and give training to select password such that the selected password will be very difficult to trace for unauthorized user or intruder. Also need to keep password private and password remembering method.
-Clearly convey mandate, roles and responsibilities of every employee in an organization.

3.To secure workstations and servers from intentional or accidental disclosure some suggestions on the basis of findings are-
-Install fire alarm systems with emergency power off systems.
-Install smoke detectors, air conditioning, humidity and dehumidification equipments, access control devices, motion detectors and Intrusion alarms on all accessible openings.
-Install Dry powder as well as CO2 type fire extinguishers.
-Appoint guard at restricted areas like server room and backup room.
-Maintain entry and exit records for visitors to each department and also escort the visitor up to the concern personnel.

4.Revoke the access to the system immediately when any employee is terminated or leaves for any reason.

5.Design a software which helps to –

-Take data backup or send data on network in encrypted form.
-Restore backuped data in normal form.
-Limit a number of concurrent sessions for a given user.
-Auto logoff/lock capabilities after predetermined time of inactive.
-Intimate newly logged user or attempts of unauthorized access.
-Create log files for manipulation of sensitive data.
-Generate audit logs for un-authored access attempts or manipulation of data containing details about date, time, changes made and user ID when an event occurs.

6.Take daily backup of data in duplicates with encrypted form using standard cryptographic algorithm. Also retain minimum 2 generations of backups at offsite safe location away from magnetic media and server room with relevant label and number for easily identification.

7.Proper insurance coverage should be taken care of against any type of risk.

8.Senior management should clearly provide healthy management support (like sufficient funding, arraigning security trainings, appreciation systems to carryout EDP activities effectively, establish appropriate policies, procedure and control.)

12 FURTHER WORK

Researcher purports statements for further research based on present study. The studies mentioned bellow of computer security maintenance may help to take any business organization on the success of developing horizon.

-Design and development of Computer Security policies suitable to changing global business environment.
-A study on manpower development on the basis of education, training in the light of computer security control and maintenance.

REFERENCES:

[1].Peltier T. R. (2002), *"Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management", New York: Auerbach Publications.*
[2].Basta A., Halton W. (2009), *"Computer Security- Concepts, Issues and Implementation", New Delhi: Course technology/cengage Learning.*
[3].Whitman M. E. & Mattord H. J. (2007), *"Principles of Information Security" (2nd ed.), New Delhi:*

Thomson Learning/Course Technology.
[4].Kothari C. R. (2004), *"Research Methodology, Methods and techniques" (2nd ed.), New Delhi: New age International (p) Ltd.*
[5].Weber R. (2007), *"Information Systems Control and Audit" (5th ed.), New Delhi: Pearson Education.*
[6]."Sugar Statistics- Maharashtra", *Retrieved December 17, 2009 from http://www. vsisugar.com/india/statistics/ maharashtra_statistics.htm*
[7]."History of Sugar", Retrieved February 27, 2009 from http://en.wikipedia. org/wiki/History_of_sugar
[8].Wood C. C. (2005), *'Information Security Roles and Responsibilities Made Easy' (Ver. 2). Information Shield, Inc. Reviewed November 15, 2009* from http://www.informationshield.com.
'[9].The Information Security Policies / *Computer Security Policies Directory', Retrieved November 7, 2009 from http://www.information-security-policies-and standards.com*

Mr. Babasaheb J. Mohite working as Assistant Professor at Sinhgad Institute of Business Management (MCA), Kamlapur-Sangola (MS), India. His area of interest is Information Security Audit & Control. Accordingly he has acquired the qualification of B.Sc., MCM, MCA, M.Sc. (Sub.Com.), M.Phil. and currently submitted Ph.D. in Computer Applications from Shivaji University, Kolhapur. He has more than thirteen years experience in the field of Industry and Academics. He has presented & published number of research papers in National & International conferences and journals. He has authored four books for BCA & BCS course.