# A Study on Problems in Implementing IT Security with Special Reference to Selected Co-operative Units

*Prof. Babasaheb J. Mohite*
*Sinhgad Institute of Business Management,*
*Kamalapur, Sangola.*
*Email Id.* bjmohite@gmail.com

***ABSTRACT-Earlier, the 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 security, every IT user must know the benefits and losses of computer security, threats to computer data and different security controls and policies required to maintain data security.***

**KEYWORDS-** ***Biometrics, Fire extinguisher, Hacking, Integrity, Virus.***

## I. INTRODUCTION

Security measures were taken to prevent or minimize the loss after the attack of any type of danger with minimum loss of assets [1]. Knowing about major possible threats to any system is important, but understanding ways to defend against these threats is equally critical due to some reasons like -

- Hundreds of possible threats exist and the cost of preventing hazards can be very high.
- System resources may be situated in different locations.
- Many persons use system assets.
- Rapid technological changes make some control obsolete as soon as they are installed.
- Many criminals who were caught but did notpunish.Therefore,organizing an appropriate defense system is one of the major activities of any functional managerwho controls any system resources [2]. Like any other systems, Information system is subjected to different threats. So to prevent or minimize the expected loss of data from those threats, security measures should be implemented.

## II. PROBLEM STATEMENT

In view of the above, the present work entitled "A Study on Problems in Implementing IT Security with Special Reference to Selected Co-operative Units" has come up for further in-depth study.

## III. OBJECTIVES OF THE STUDY

1. To study and analyze the data security measures adopted by the organization.
2. To examine the awareness level among users about the benefits or losses of data security.
3. To suggest measures for efficient Information Security.

## IV. HYPOTHESIS

1. Units do not differ significantly in awareness of different security measures in the vicinity.

2. Measurement of the present scenario of the awareness level of the data security is not implemented by the users.

## V. SCOPE OF THE STUDY

The study was focused on co-operative units of the Warana Business Group, Karad, Maharashtra, India for collection of data. The Therefore the scope is limited to a sample size was 69 comprising of three units. The study is aimed at comparing the security awareness, security measures implemented and threats experienced by the Users.

## VI. VALIDITY OF THE STUDY

1. Present research focus on the current situation of computerization and data security measures adopted at different units of the Warana Business Group.
2. Awareness of security plays an important role in securing valuable assets of the organization.
3. Research factors that helpthe organization in deciding the security policies regarding the data security.

## VII. METHODOLOGIES ADOPTED

In order to study the selected problem in details, the researcher has made use of different resources to collect the reliable information pertaining to data security systems used in the following units of the Warana Business Group.

- Warana Co-operative Sugar Factory Ltd. Karad, Maharashtra India.
- Warana Co-operative Milk Produce Processing Society Ltd.,Karad, Maharashtra India.
- Warana region Co-operative Customer care unit

The researcher has collected both primary and secondary data regarding the present study [3]. Primary Data: Researcher has prepared a questionnaire based on a set of objectives. Secondary Data: The secondary data related to data security was collected from various books, related journals, magazines and websites. The secondary data in respect of profile of the company were collected from company files, magazines etc.

***Sampling Method:*** Presently, the Warana co-operative complex runs successfully 25 cooperative units. Out of this researcher has chosen above said three co-operative units. These units have been selected on the basis of the following parameters-

- The unit has more than 10 computers.
- A unit having more than 80% computers in network.
- A unit having different sections or sub-units.
- The unit has more than 25 computer users.

***Sampling technique***

For the present research worthe proportionate convenience sampling techniqueque is used and accordingly out of the total 311 IT users, 62 users representing 20% of the universe have been considered as a sample. The method thus considered is convenience sampling because during the present research work, while collecting data, those respondents who were willing to take part in the research study and prepared to divulge with the required information were finalized. This process was continued till the sample size of 62 was arrived at.

***Breakup of sampling size-***

| Organization | IT Users | 20% Proportion |
|---|---|---|
| Warana Milk Group | 152 | 30 |
| Warana Sugar Factory | 128 | 26 |
| Warana Market | 31 | 6 |
| **Total** | **311** | **62** |

## VIII. LIMITATIONS

a. The conclusion drawn from the survey is limited to three units of the Warana Business Grouponly.
b. Many respondents were not able to answer the questions regarding the technical aspects of threats and measures of security. So the researcher had to trace out the problem by using some technicalknowledge, skill, experience, and by

questioning to respondents regarding the required details.

## IX. DATA ANALYSIS

| Antivirus updated regularly? ↓ | Organizations | | | | | |
|---|---|---|---|---|---|---|
| | Milk Group | | Sugar Factory | | Market | |
| | No. of IT Users | Percent | No. of IT Users | Percent | No. of IT Users | Percent |
| Yes | 15 | 50.00 | 16 | 61.54 | 4 | 66.67 |
| No | 4 | 13.33 | 3 | 11.54 | 0 | 0.00 |
| To some extent | 11 | 36.67 | 7 | 26.92 | 2 | 33.33 |
| **Total** | 30 | 100.00 | 26 | 100.00 | 6 | 100.00 |

Table1: Antivirus Updation Status

Above table implies that, majority of respondent's updates Antivirus programs regularly.

| Training is necessary ↓ | Organizations | | | | | |
|---|---|---|---|---|---|---|
| | Milk Group | | Sugar Factory | | Market | |
| | No. of IT Users | Percent | No. of IT Users | Percent | No. of IT Users | Percent |
| Yes | 29 | 96.67 | 25 | 96.15 | 6 | 100.00 |
| No | 1 | 3.33 | 1 | 3.85 | 0 | 0.00 |
| **Total** | 30 | 100.00 | 26 | 100.00 | 6 | 100.00 |

Table 2: Necessity of IS Security Training

Table 2 depicts that, majority of employee's strongly agree for training on maintaining data security is very important and essential.From the table, it is observed that, out of total Respondents from all units under study majority of respondents use CD/DVD as a main backup medium.Similarly, out of total respondents from all units 10 to 25% of respondents use Zip/USB disk, Pen drive as Backup server on Network as a backup medium, At the backup server on Network as a backup medium, At the same time, not a single respondent uses Magnetic tape as a storage medium to store backup data in their organization.All units are having facility to validate input data through application programs. On the other hand in all these units, there is a negative response towards -

- Facility to intimate newly logged user.
- Maintain a log file for sensitive data.
- Background checks on selection of IT staff.
- Data security officer appointment.
- Formal disciplinary process for staff that violates

| Security policies. Threat experienced in Organization ↓ | Organizations | | | | | |
|---|---|---|---|---|---|---|
| | Milk Group | | Sugar Factory | | Market | |
| | No. of IT Users | Percent | No. of IT Users | Percent | No. of IT Users | Percent |
| Theft of Computer Hardware | 5 | 5.43 | 3 | 4.05 | 1 | 5.56 |
| Theft of Software | 0 | 0.00 | 0 | 0.00 | 0 | 0.00 |
| Virus | 29 | 31.52 | 25 | 33.78 | 6 | 33.33 |
| Hardware Fault | 20 | 21.74 | 20 | 27.03 | 4 | 22.22 |
| Hacking | 0 | 0.00 | 0 | 0.00 | 0 | 0.00 |
| Human negligence | 28 | 30.43 | 19 | 25.68 | 5 | 27.78 |
| Environmental Hazards | 8 | 8.70 | 5 | 6.76 | 1 | 5.56 |
| Data alteration | 2 | 2.17 | 2 | 2.70 | 1 | 5.56 |
| **Total** | 92 | 100.00 | 74 | 100.00 | 18 | 100.00 |

Table 3: Disaster Experienced by Employees

| Backup taken on ↓ | Organization | | | | | |
|---|---|---|---|---|---|---|
| | Milk Group | | Sugar Factory | | Market | |
| | No. of IT Users | Percent | No. of IT Users | Percent | No. of IT Users | Percent |
| Backup Server on N/W | 7 | 11.11 | 6 | 13.04 | 0 | 0.00 |
| Zip / USB Disks | 15 | 23.81 | 10 | 21.74 | 1 | 12.50 |
| Magnetic tape | 0 | 0.00 | 0 | 0.00 | 0 | 0.00 |
| CD/DVD | 27 | 42.86 | 22 | 47.83 | 5 | 62.50 |
| Pen Drive | 14 | 22.22 | 8 | 17.39 | 2 | 25.00 |
| Total | 63 | 100.00 | 46 | 100.00 | 8 | 100.00 |

Table 4: Media Used For Data Backup

| System | Organization & IT Users Response | | | | | |
|---|---|---|---|---|---|---|
| | Milk Group | | Sugar Factory | | Market | |
| | Yes | No | Yes | No | Yes | No |
| Facility to intimate newly logged user | 0 | 3 | 0 | 3 | 0 | 1 |
| Maintain log files for sensitive data | 0 | 3 | 0 | 3 | 0 | 1 |
| Facility to validate input data | 3 | 0 | 3 | 0 | 1 | 0 |
| Conduct background check on selection of IT staff | 0 | 3 | 0 | 3 | 0 | 1 |
| Appointed data security officer | 0 | 3 | 0 | 3 | 0 | 1 |
| Formal disciplinary process for staff that violate security policy | 0 | 3 | 0 | 3 | 0 | 1 |
| Maintained security plan and policies | 0 | 3 | 0 | 3 | 0 | 1 |
| Any biometric measure | 0 | 3 | 0 | 3 | 0 | 1 |
| Security control tested regularly | 0 | 3 | 0 | 3 | 0 | 1 |

Table 5: Security Controls Used

| Security facilities | Organization & IT Users Response | | |
|---|---|---|---|
| | Milk Group | Sugar Factory | Market |
| Fire Alarm System | 0 | 0 | 0 |
| Smoke Detectors | 0 | 0 | 0 |
| Fireproof Ceiling, doors and furniture | 3 | 3 | 1 |
| A.C. and Humidity measuring Equipment | 3 | 3 | 1 |
| Access Control Device | 0 | 0 | 0 |
| Motion Detectors | 0 | 0 | 0 |
| Intrusion Alarm on all accessible openings | 0 | 0 | 0 |
| Separate arrangement for electricity and N/W cable | 3 | 3 | 1 |
| Fire Extinguisher | 3 | 3 | 1 |
| Appointed Watchman | 0 | 0 | 0 |
| Maintained entry and exit record for visitors | 0 | 0 | 0 |

$H_0$: Units do not differ significantly in awareness of different security measures in the vicinity

$$SSE = \sum_{i=0}^{n}\sum_{j=0}^{c}(x_{ij} - \overline{X_j})^2$$

$$= (0-1.090)^2 + (0-1.090)^2 + (3-1.090)^2 + \ldots\ldots\ldots + (1-0.3636)^2 + (0-1.036)^2$$

$$=14.9091+14.9091+2.5454$$

$$=32.3636$$

**SSE = 32.3636**

$$SST = \sum_{i=0}^{n}\sum_{j=0}^{c}(x_{ij} - \overline{X})^2$$

$$= (0-0.8484)^2 + (0-0.8484)^2 + \ldots\ldots + (1-0.8484)^2 + \ldots..$$

$$=52.2419$$

**SST = 52.2419**

**Degrees Of Freedom**

dfc = c-1 = 3-1 = 2 dfe = N-C = 33-3 = 30

dft = N-1 = 33-1= 32

**Mean Sum of Squares**

$$MSC = \frac{SSC}{dfc} = \frac{3.870177}{2} = 1.935885$$

**M S C = 1.935885**

$$MSE = \frac{SSE}{dfc} = \frac{32.3636}{30} = 1.07878$$

**M S E = 1.07878**

**Here we use 'F' test, since MSC > M SE**

F test = $\frac{1.935885}{1.07878} = 1.7945$ at (2, 30) degrees of

| Sources of Variance | d.f | s.s | M.S.S | F Test |
|---|---|---|---|---|
| Between | 2 | 3.870177 | 1.935885 | 1.7945 |
| Error | 30 | 32.3636 | 1.07878 | |
| Total | 28 | 52.2419 | | |

ANOVA Table

Table value for **F ratio** for (**2,30)** d.f. is **3.32** Thus calculated value is less than given table value, gives the conclusion that Organizations do not differ significantly [3].

Using Yale's correlation, using the Pooling techniques

$$\chi^2 = \sum_{i=0}^{n} \frac{(O_i - E_i)^2}{E_i} = 0.043036$$

Table value for $\chi^2$For**8 degrees of freedom** at the 5% level of significance is **2.73.**

Researcher accepts the hypothesis that, Measurement of the present scenario of the awareness level of the data security is not implemented by the users [3].

| **Security Measures** | **Yes** | **No** |
|---|---|---|
| Security training programs | 0 | 62 |
| Signed confidential agreement | 0 | 62 |
| Sufficient password length set | 17 | 45 |
| Got training about privacy of password | 0 | 62 |
| Use of fire extinguisher | 7 | 55 |
| Installation of Antivirus program | 62 | 0 |
| Upadation of Antivirus regularly | 30 | 12 |
| Scanning of secondary storages | 57 | 5 |
| Having unique logon & a private area of data store | 0 | 62 |
| Auto log off or lock capability | 56 | 6 |
| Screen saver password facility | 37 | 25 |
| Deletion of internet cookies | 16 | 46 |
| Database backup facility | 49 | 13 |
| $H_0$: - Measurement of the present scenario of the awareness level of the data security is not implemented by the users | | |

## X. FINDINGS

1. All the units under study do not have facilities like- Fire alarm system with emergency power off system, smoke detectors, fireproof ceilings, doors and furniture's, access control device, motion detectors, intrusion alarms at all accessible openings, watchman at server & backup room. Also they can't maintain entry and exit records for visitors to the department.
2. In all organization fire extinguishers mainly of $CO_2$ type is installed, but very few employees know how to use the fire extinguisher systems.
3. It is found that, in all organization individual computers used by more than one user with unique username and password.
   - Not a single organization has security controls implemented, such as–
   - Facility for intimate newly logged users.
   - Staff signatures on a confidentiality agreement about data security.
   - Background checks on selection of IT staff.
   - Appointment of data security officer.
   - Any formal security plan and policies as well as a disciplinary process for staff that violates data security policies and procedures.

## XI. SUGGESTIONS

To carry out proper and rigid security plans some suggestions on the basis of findings are as follows, organizations should –

1. Implement firewall to secure the network from the outside world or unauthorized requests.
2. Use Server Operating systems like Linux which is more secure from virus attack.
3. Use workstations operating system which has inbuilt firewall facility instead of using the Windows 98 operating system.
4. All organizations are having Internet facilities and installed antivirus software's on all machines.
5. Regularly schedule for updates to the antivirus software's against the latest viruses and spam.
6. Install different latest patches and service packs of system and application software's.
7. Delete internet cookies after every visit of Internet.
8. Conduct the background check on a selection of IT staff.
9. Create separate logins for each user and allocate a private area for data storage.
10. Make compulsory or arrange conferences, refreshers, trainings or seminars on essentials of data security like data security policies and procedures.
11. Get signed on a confidential agreement about data security.
12. To secure workstations and servers from intentional or accidental disclosure some suggestions on the basis of findings are-

13. Install Dry powder as well as $CO_2$ type fire extinguishers.
14. Maintain entry and exit records for visitors to each department and also escort the visitor up to the concern personnel.
15. Appoint a data security officer from Corporate Internal Audit department to design and validate security plans and policies. And also to conduct formal risk management activities and regularly test the security controls implemented.
16. Take daily backup of data in duplicates with encrypted form using standard cryptographic algorithm. Also retain minimum 2 generations of backups at an off-site safe location away from magnetic media and server room with relevant label and number for easy identification.

## REFERENCES:

[1] Thomas R. Peltier (Book) titled "Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management", Auerbach Publications [2002].

[2] Alfred Basta, Wolf Halton (Book) titled "Computer Security- Concepts, Issues and Implementation", Cenage Learning India Edition [2009].Michael E. Whitman and Herbert J. Mattord (Book) titled "Principles of information Security", Thomson Learning- Course Technology, Second Edition [2007]

[3] Ron Weber, Information Systems Control and Audit, Pearson Education, Fifth edition [2007]