Delhi Business Review ≤ Vol. 3, No. 2, July - December 2002

CONTINGENCY PLANNING FOR MANAGING COMPUTER DISASTERS

A STRATEGIC SUPPORT TO HUMAN RESOURCES IN SOFTWARE INDUSTRY

Subhash C. Kundu
Deepika Jain

COMPUTERIZED systems are vulnerable to theft, damage, disruptions, or misuse. The proper use and cooperation of information systems depends not only on technical, organizational and design factors but also on the behaviour of people. Computer disasters include theft, virus, malicious damage, hardware faults, hacking, environment, software, communications, human error or negligence, natural disasters, etc. These disasters affect efficiency and effectiveness of systems and human resources. To remain efficient and effective, organizations have to adopt a proactive approach to manage crisis caused by computer disasters. Proactive approach to crisis management includes forecasting potential crises and planning to deal with them. Generally, organizations have time and resources but they do not have orientations for adopting contingency planning to deal with crises. So, an effort has been made in this study to find out the human, organizational, and technological context in which an organization operates and how organizations are developing or incorporating system of contingency planning for managing computer disasters. The study is based on primary data gathered with the help of a questionnaire containing 29 statements regarding contingency planning for managing computer disasters. In all 102 fully filled up questionnaires were gathered from executives of ten software companies and analyzed by applying statistical techniques i.e. factor analysis, means and grand means. Cronbach alphas regarding scale and sub-scales were found very high. The present study has extracted six components regarding contingency planning adopted by Indian and multinational software companies operating in India for managing computer disasters and supporting human resources strategically in crises. The components derived are strategic efforts, technical and structural support, organizational preparedness and training, evaluation and diagnosis efforts, organizational awareness and communicational efforts, and stress management and psychological support. MNCs are stronger than the Indian companies on strategic efforts, technical and structural support. Again MNCs are more serious on the third dimension i.e. organizational preparedness and training of employees. Both are doing well in the case of evaluation and diagnosis of various aspects of contingency planning. Indian companies are comparatively stronger in awareness and communicational efforts. Both Indian and MNCs are equally strong in managing stress and providing support to employees in crises.

Introduction

Computerized systems are vulnerable to theft, damage, disruptions, or misuse (www.cs.mdx.ac.uk, 20002). The proper use and operation of information systems depends not only on technical, organizational and design factors but also on the behaviour of people. The critical role played by automated information systems in business, government and daily life requires special steps to protect them and to ensure that they are accurate and reliable. Valuable data can be destroyed if computer hardware malfunctions or if any one tampers with computerized files. More specifically computer disasters include theft, virus, malicious damage, hardware faults, hacking, environment, software, communications, human error or negligence, natural disasters, etc. These disasters affect efficiency and effectiveness of systems and human resources. Companies may loose much money every hour or day if their systems are not working well.

To remain efficient and effective, organizations have to adopt a proactive approach to manage crisis caused by computer disasters. Proactive approach to crisis management includes forecasting potential crises and planning to deal with them. Generally, organizations have time and resources but they do not have orientations for

adopting contingency planning to deal with crises. So, an effort has been made in this study to find out the human, organizational, and technological context in which an organization operates and how organizations are developing or incorporating system of contingency planning for managing computer disasters.

Causes of Disaster

Disaster is an event that causes permanent and substantial damage or destruction to the property, equipment, information, staff or services of the business (Dorey, 1991). A crisis is an abnormal situation which presents some extra-ordinary high risks to a business and which will develop into a disaster unless carefully managed (Caelli, Longley and Shain, 1991). Many times organizations may suffer from disasters. Most serious causes of a disaster *(http://peoplenetscape.com/...htm)* are given below with brief comments:

Theft	-	Theft of PCs and small systems
Virus	-	Organizations run a 6% risk of virus infection annually, cost of recovery is high.
Malicious damage	-	Including software 'time bombs' as well as physical.
Hardware faults	-	Mid-range systems are significantly more prone to them.
Hacking	-	This may underestimate the problem; prosecutions are the exception and many cases go unreported.
External Environment	-	Power problems are the primary cause; air conditioning failures are significant.
Software	-	Software problems
Communication	-	Several major switch failures occurred. LAN failure is an increasing issue.
Human error or negligence	-	Error, negligence or criminal behaviour.
Natural disasters	-	Includes hurricanes, natural floods, etc.
Fire	-	A major cause of physical disaster.
Flood	-	Excludes natural floods. Includes damaged pipes; flood from adjacent fire fighting, etc.

Contingency Planning

Creating a plan may minimize the disruption of operations and ensure some level of stability and an orderly recovery after a disaster. The plan is the road map from disaster to recovery. The planning process should also include a detailed study of disaster recovery alternatives. Contingency planning aims at getting back as soon as possible to 'business as usual' or in other words to come back rapidly to the situation experienced prior to crisis and it should also lead to the realization that the managers of an organization have a moral and social responsibilities towards themselves, the organization, the stakeholders and the society in general (Pauchant*et al.* 1991).

A contingency plan is developed to provide the best possible recovery capabilities in the event that security measures were not effective and some loss of capability or data has occurred. One of the values of contingency plan is that planning has taken place before the contingency event and therefore, valuable recovery time is not lost in planning after the fact *(www.dis.state.ar.us/...htm).*

The three hierarchical functions to contingency planning are business continuity planning, disaster recovery planning and emergency management planning. The breakdown of these functions is based on the role they play with contingency planning. Although most organizations address all three functions in one plan, it is important to recognize that each serves a different function *(www.dis.state.ar.us/...htm).*

Literature Review

Parnell *et al.* (1997) in their study examines the crisis management awareness patterns among Egyptian managers. Managers were asked to relate their degree of concern on 21 major crisis events and to provide the frequency of these events in their respective organizations. Results suggested that executives considered the perceived controllability and sources of crisis (i.e. internal or external) when planning for crisis contingencies. Further they found that computer breakdowns were the most frequent crisis event within 53 organizations reporting the occurrence.

JLJ consulting services (2000) conducted a security survey and found that about all respondents were found concerned about security and the respondents identified specific areas of concern like viruses, hackers, hardware and network.

Pauchant *et al.* (1991) found in their study that contingency planning efforts can be grouped in five specific but interrelated clusters. These are:

- ✍ Strategic efforts
- ✍ Technical and structural efforts
- ✍ Evaluative and diagnosis efforts
- ✍ Communicational efforts
- ✍ Psychological and cultural efforts.

This coverage of contingency planning according to Pauchant*et al.* (1991) tries to achieve the aims like developing a systematic plan, ideologies of reference, including the overall corporate philosophy, the concept of corporate excellence, and the ability to view an organization as both a productive and destructive system.

Objectives

The main objective of the study is to assess the impact of strategic and contingency planning in the management of computer disasters for developing a support system to human resources. To achieve the main objective, the following are set as sub objectives.

i) To know the degree of adopting the contingency planning and its impact on disaster management.

ii) To know about the role and support of top management in disaster management.

iii) To assess the strategic efforts put in by the organizations.

iv) To assess the organizational efforts for supporting human resources in crises.

v) To compare the MNCs and Indian software companies on the issue.

Methodology

This study is based on primary data gathered with the help of a questionnaire developed for the purpose. In all 29 statements regarding contingency planning for managing computer disasters were incorporated in the questionnaire. These statements were taken on five point scale ranging from one to five. The respondent executives were required to rate the statements on a five point rating scale where one indicated that the respondents were strongly disagree, two meant disagree, three meant neutral, four indicated agree and five meant strongly agree about what was described in the statement.

The questionnaires were administered to the executives (software developers) of ten software companies operating in North India, out of that four were multinational companies. Fifteen questionnaires were distributed to at least fifteen executives of each of the ten companies. At least 10-11 filled up questionnaires from each company were ensured and received. So, in all 102 fully filled up questionnaires could be gathered, those were finally processed for analysis. The sample distribution is as shown in Table 1.

Table 1: Sample Distribution

Type of Software Co.	*No. of Co.*	*No. of Executives Surveyed*
Indian	6	61
Multinational	4	41
Total	**10**	**102**

The statistical methods like factor analysis, mean and grand mean scores were used to bring out the results. Cronbach alphas were also calculated to see the reliability of scale and sub-scales.

Results

Data were subjected to principal components factor analysis with varimax rotation by using the criterion that components (factors) with eigen value greater than 1.00 were retained. For factor clarity, loadings exceeding 0.55 were considered for determining factors. However, Harman (1976) outlined the procedure for approximating standard error of factor loadings i.e. loadings greater than 0.29 are significant at 0.05 level. The values of communalities (h^2) ranged from 0.60 to 0.86 for various variables. It means factor analysis has extracted good amount of variance in the variables. Further the data were analyzed by making use of means and grand means. Scale value of means were also calculated for further analysis. Mean scores were used to assess the extent of adopting the contingency planning for managing computer disasters and comparing the Indian software companies and multinationals on the issue in context.

Table 2 shows extracted factors, variable loadings, eigen values, and percentage of variance explained by each factor. Factor analysis yielded six factors accounting for 74.61 per cent of total variance. Factor 1 named as *strategic efforts* consisted of eight variables and explained 40.14 per cent of the variance. This is the first and most important factor on which two variables were loaded highly i.e. adopting new communication technologies with time and strong management commitment to contingency planning for managing disasters. Other variables like interaction with external environment, practicing of contingency planning, changing of emergency policies and manuals, clarity of management about the impact of crisis on human dimensions, providing information, and integration of contingency planning into strategic planning process were also loaded significantly. It reflected the extent of strategic efforts of organizations towards contingency planning for managing computer disasters.

Factor 2 labeled as *technical and structural support* consisted of eight variables. Dedicated budget for contingency planning, and developing emergency policies and manuals were the two variables those loaded on the factor at the highest order. Portfolio strategies, maintaining separate crisis management unit, simulation exercises for employees, frequent help of outside experts, pursuing dedicated research on potential hidden dangers, and system of early warning signals were other important variables that loaded significantly. This factor indicated the technical and structural support system developed by the companies to help human resources for managing crisis.

Factor 3 *organizational preparedness and training*, focused on the preparedness of the organization and training of employees for managing computer disasters. In all, four variables were loaded on the factor those were having appropriate changes in corporate philosophy, integration of contingency planning into corporate excellence, training and workshops of executives, and continuously reviewing of security norms.

Factor 4 named as *evaluation and diagnostic efforts* consisted of three variables i.e. legal and financial audit of threats and liabilities, regular modifications in the insurance coverage, and the acceptance of whistle blowers. These variables focused on evaluative efforts of the organization.

Factor 5 labeled *Organizational awareness and communicational efforts* consisted of three variables and explained 4.49% of the variance. The variables loaded on the factor were computerized inventories, increased collaboration and lobbying among stakeholders, and aware about the existence of criminal behaviour in the organization.

Table 2: Variable Loadings of Contingency Planning for Managing Computer Disasters for the Varimax Rotated Principal Components (N=102)

Factors	*Loadings*	*Eigen Value*	*% of Variance*
Factor 1 (Strategic Efforts)			
Practicing of contingency planning	0.73	11.64	40.14
Integration of contingency planning into strategic planning process	0.64		
Changing of emergency policies & manuals according to requirements	0.69		
Interaction with external environment including media to develop public relations	0.76		
Providing information about security and crisis management to every component	0.65		
Adopting new communication technologies with time	0.84		
Strong management commitment to contingency planning	0.79		
Management is clear about the impact of crisis on human dimensions	0.66		
Factor 2 (Technical and Structural Support)			
Employees are made to go through crisis simulation exercises	0.66	3.91	13.47
Portfolio strategies are being used to manage the diversified crisis	0.77		
There is separate crisis management department	0.72		
The emergency policies and manuals are developed	0.79		
The services of outside experts are used frequently for developing contingency planning	0.64		
There is dedicated budget for crisis management/contingency planning.	0.85		
There is a system of early warning signals detection and scanning in the organization	0.59		
Company pursues dedicated research on potential hidden dangers	0.64		
Factor 3 (Organizational Preparedness and Training)			
Appropriate changes have been made in the corporate philosophy for disaster management	0.55	2.06	7.09
Contingency planning has been integrated into corporate excellence	0.62		
Training and workshops are conducted regularly	0.69		
Company continuously reviews the security norms	0.74		
Factor 4 (Evaluation and Diagnosis Efforts)			
Legal and financial audit of threats and liabilities are carried out by the organization	0.73	1.49	5.13
Modifications in the insurance coverage are done on regular basis	0.76		
There is improved acceptance of "Whistle Blowers"	0.57		
Factor 5 (Organizational Awareness and Communication Efforts)			
Computerized inventories of employees, events, products, capabilities, etc. are being maintained	0.60	1.30	4.49
Increased collaboration or lobbying among stakeholders for security purposes	0.79		
The management is aware about the existence of any criminal behaviour in the organization	0.57		
Factor 6 (Stress Management and Psychological Support)			
The management is aware about the existence of any criminal behaviour in the organization.	0.56	1.24	4.28
Employees are provided with psychological support during crisis	0.62		
Management properly manages stress and anxiety during crisis	0.89		

Finally, factor 6, stress management and psychological support, consisting of three variables focused on managing stress and anxiety and providing psychological support to employees during crises. Management was also aware about the criminal behaviour of employees in the organization.

Table 3 shows the mean scores, grand mean scores, total mean value of the factor, and scale (sub scales) value of the mean. Mean scores of each variable for Indian and multinational companies are calculated and compared. Grand means were used to see the overall practice of the contingency planning. According to table 3, mean scores of various variables regarding strategic efforts show both Indian and multinational companies are doing strategic

Table 3: Mean and Grand Mean Scores of Various Variables Regarding Contingency Planning for Managing Computer Disasters

Factor Variables	***Indian Co. Mean Scores***	***MNCs Mean Value***	***Grand Means***
Factor 1 (Strategic Efforts)			
Practicing of contingency planning	3.52	4.05	3.79
Integration of contingency planning into strategic planning process	3.34	4.02	3.68
Changing of emergency policies and manuals according to requirements	3.02	3.73	3.38
Interaction with external environment including media to develop public relations	3.44	4.15	3.80
Providing information about security and crisis management to every component	3.08	4.10	3.59
Adopting new communication technologies with time	3.93	4.49	4.21
Strong management commitment to contingency planning	3.10	4.02	3.56
Management is clear about the impact of crisis on human dimensions.	3.59	3.85	3.72
Total Mean Value	**27.02**	**3.38**	**32.41**
Scale Value of Mean	**4.05**	**29.73**	**3.72**
Factor 2 (Technical and Structural Support)			
Employees are made to go through crisis simulation exercises	2.98	3.22	3.10
Portfolio strategies are being used to manage the diversified crisis	3.23	3.39	3.31
There is separate crisis management department	2.72	3.24	2.98
The emergency policies and manuals are developed	3.43	3.83	3.63
The services of outside experts are used frequently for developing contingency planning	3.28	3.80	3.54
There is dedicated budget for crisis management/contingency planning	3.34	3.68	3.51
There is a system of early warning signals detection and scanning in the organization	3.31	4.12	3.72
Company pursues dedicated research on potential hidden dangers	3.61	3.71	3.66
Total Mean Value	**25.90**	**3.24**	**28.99**
Scale Value of Mean	**3.62**	**27.45**	**3.43**
Factor 3 (Organizational Preparedness and Training)			
Appropriate changes have been made in the corporate philosophy for disaster management	3.74	4.24	3.99
Contingency planning has been integrated into corporate excellence	3.54	4.02	3.78
Training and workshops are conducted regularly	3.67	3.41	3.54
Company continuously reviews the security norms	4.07	4.05	4.06
Total Mean Value	**15.02**	**3.76**	**15.72**
Scale Value of Mean	**3.93**	**15.37**	**3.84**

Factors Variables	*Indian Cos Mean Scores*	*MNCs Mean Value*	*Grand Means*
Factor 4 (Evaluation and Diagnosis Efforts)			
Legal and financial audit of threats and liabilities are carried out by the organization	3.70	3.88	3.79
Modifications in the insurance coverage are done on regular basis	3.64	3.63	3.64
There is improved acceptance of "Whistle Blowers".	2.97	3.08	3.03
Total Mean Value	**10.31**	**3.44**	**10.59**
Scale Value of Mean	**3.53**	**10.46**	**3.49**
Factor 5 (Organizational Awareness and Communicational Efforts)			
Computerized inventories of employees, events, products, capabilities, etc. are being maintained	4.23	4.12	4.18
Increased collaboration or lobbying among stakeholders for security purposes	3.69	3.37	3.53
The management is aware about the existence of any criminal behaviour in the organization	4.12	3.60	3.86
Total Mean Value	**12.04**	**4.01**	**11.09**
Scale Value of Mean	**3.70**	**11.57**	**3.86**
Factor 6 (Stress Management and Psychological Support)			
The management is aware about the existence of any criminal behaviour in the organization	4.12	3.60	3.86
Employees are provided with psychological support during crisis	3.31	3.79	3.55
Management properly manages stress and anxiety during crisis	3.75	3.89	3.82
Total Mean Value	**11.18**	**3.73**	**11.28**
Scale Value of Mean	**3.76**	**11.23**	**3.74**

efforts for managing computer disasters. But MNCs are putting in greater efforts than Indian software companies. Scale value of mean for Indian companies is 3.38 and for MNCs is 4.05. The mean scores pattern indicates that MNCs (x = 3.62) are providing comparatively more technical and structural support to executives as compared to Indian (x = 3.24) software companies. Further both Indian (x = 3.76) and MNCs (x = 3.93) are more or less equally strong on the variables relating to organizational preparedness and training of employees. Again the mean scores pattern shows that both Indian and multinational software companies are equally stressing on evaluative and diagnostic variables except one i.e. whistle blowing. Whistle blowing (x = 2.97) is not acceptable in Indian software companies. Both Indian and MNCs more or less are on equal footing regarding variables computerized inventories and collaboration. But Indian organizations are more aware about the criminal behaviour in the organization. Indian and multinational companies are equally stressing on stress management. But psychological support to employees during crises is more prominent in the case of MNCs (x = 3.79) than Indian companies (x = 3.31).

Table 4 presents total (factor) mean values, scale (sub-scale) value of mean (i.e. total mean value divided by the number of variables), standard deviations, Cronbach alpha of full scale (29 variables), and Cronbach alphas of different factors (sub-scales). The scale value of mean for each factor shows the prevalence of the factors. A perusal of table 4 indicates that two factors i.e. awareness and communicational efforts and organizational preparedness & training were maximum prevalent, followed by strategic efforts and stress management & psychological support. The extent of the prevalence of technical and structural support factor was least. Cronbach alphas were high for the full scale and all sub scales.

Table 4: Summary Table of Means and Cronbach's Alpha for Various Factors of Computer Disaster Management

Factors	*No. of Items*	*Total Mean Values*	*SD*	*Scale Value of Mean*	*Cronbach Alphas of Sub scales*
Strategic efforts	8	29.73	0.24	3.72	0.93
Technical and Structural Support	8	27.45	0.27	3.43	0.92
Organizational preparedness and training	4	15.37	0.23	3.84	0.81
Evaluation and diagnosis efforts	3	10.46	0.40	3.49	0.66
Awareness and communicational efforts	3	11.57	0.32	3.86	0.67
Stress management and psychological support	3	11.23	0.17	3.74	0.59
Cronbach Alpha of the full scale (29 items)					0.94

Discussion and Conclusion

The present study has extracted six components regarding contingency planning adopted by Indian and multinational software companies operating in India for managing computer disasters and supporting human resources strategically in crises. The components derived are strategic efforts, technical and structural support, organizational preparedness and training, evaluation and diagnosis efforts, organizational awareness and communicational efforts, and stress management and psychological support. According to Pauchant, Mitroff and Lagadec (1991) contingency planning efforts for managing disasters can be grouped in five clusters those are more or less similar to our study. These groups are strategic efforts, technical and structural efforts, evaluation and diagnosis efforts, communicational efforts and psychological and cultural efforts. However, numbers of variables included by Pauchant et al., (1991) in their study were 37 those were more than the present study which included 29 variables.

Strategic efforts by organizations emerged as one of the important component of contingency planning. It consists of incorporating new communication technologies, top management commitment to contingency planning, developing public relations by interacting with external environment, disseminating information about crises and security, changing policies and manuals, etc. The software companies are trying to offset the impact of computer disasters by concentrating on strategic actions. Technical and structural support has emerged another dimension of contingency planning. Providing dedicated budget for contingency planning, preparing diversified strategies, developing policies, maintaining separate crises management unit and practicing crises simulation exercises are some important ways the organizations adopt to provide technical and structural support to employees. Multinationals are much more stronger than the Indian software companies on these two dimensions of contingency planning.

Organizational preparedness & training of employees in crisis management is another way of contingency planning. This factor consists of incorporating proper changes in corporate philosophy, integrating contingency planning into corporate excellence, conducting training and workshops of employees in crisis management, and continuously reviews the security norms. Multinational software companies are more serious for adopting these practices than the Indian ones.

Evaluation and diagnosis of various aspects of contingency planning have been reported as one of the important dimensions. Indian and MNCs are doing equally well in the case of audit of threats and liabilities and modifications in the insurance coverage. They significantly differ on the issue of acceptance of whistle blowing. Whereas MNCs are accepting the practice. In the absence of this practice, Indian companies may remain unaware about their right or wrong decisions. Whistle blowing means the disclosing by an employee of illegal or unethical conduct on the part of others or management within the organization.

The fifth dimension is organizational awareness and communicational efforts which consists of computerized inventories, increased collaboration among stakeholder for security purposes, and awareness about the existence of criminal behaviour in the organization. Indian companies are comparatively stronger on this dimension as compared to MNCs.

The last important contingency planning component is stress management and psychological support. This dimension covers organizational strengths in managing stress and anxiety and management's psychological support to employees during crisis. Both Indian and MNCs are equally strong in managing stress and providing support to employees in the adverse situations.

The organizations face risks, disasters, accidents and crises in their everyday operations. Contingency planning is the way that may be helpful in solving crises. If the contingency planning can encompass the whole range of organizational risks, empower and strengthen organizational structures, communications, and making the organization more tolerable to disasters, it can be a means of organizational effectiveness and differentiation leading to better overall production minimizing risk. In such a way adopting contingency planning for managing disasters becomes one of the important steps in gaining competitive edge over other companies in the field.

References

Caelli, W., Longley, D. and Shain, M. (1991) "Information Security Handbook (Ed)" London, Mc Millan.

Dorey, P. (1991) "Contingency Planning and Damage Avoidance" In Caelli, W.; Longley, D. and Shain, M. (Ed), Information Security Handbook, London, Mcmillan.

Harman, H.H. (1976) "Modern Factor Analysis" Chicago, University of Chicago Press.

http://peoplenetscape.com/thanos/thesis/security.htm

Johnson, J. (2000) VITC's 2000. Security Survey Results and Analysis (JLJ consulting services), www.viscc.org.

Parnell, J.A., Crandall, W. and Menefee, M.L. (1997) "Management Perceptions of Organizational Crisis: A Cross Cultural Study of Egyptian Managers" Academy of Strategic and Organizational leadership Journal, Vol. 1, Nov.1, www.alliiedacademics.org.

Pauchant, T.C., Mitroff, I.I. and Lagadec, P. (1991) "Toward a systematic crisis management strategy: Learning from the best examples in the US, Canada and France" Industrial Crisis Quarterly, 5, p.209-232.

www.cs.mdx.ac.uk/staffpages/geetha/bis3000/security.html

www.dis.state.ar.us/sp/arch/policy2000/contingplan.htm

CALL FOR PAPERS

Fourth International Conference on January 8-9, 2003 at New Delhi, India

Theme

Management and Technology – Vision 2020

Technical Sessions

1. Creating Corporate Advantage in the Global Economy
2. Legal, Accounting and Financial Issues in the Cyber Age
3. Driving the Organization: The HR Way
4. Managing Innovative Technology
5. Network Marketing and E-Commerce: Emerging Dimensions

International Seminar

"Online Education and Training: Challenges and Quality Perspectives"

Key Dates

- Submission of Abstract	-	June 1, 2002
- Acceptance of Abstract to be communicated by	-	July 1, 2002
- Paper to be Received by	-	August 1, 2002
- Paper Acceptance by	-	September 16, 2002
- Fee Submission by	-	October 1, 2002

Best Research Paper Award - Details available on www.shtr.org/4ic.html

Under the joint auspices of

✍ GGS Indraprastha University

✍ Society for Human Transformation and Research

✍ Delhi School of Professional Studies and Research

Integrated Academy of Management and Technology

✍ DSPSR: Center for Information Technology

✍ SHTR Consulting Group, Delhi School of e-Learning, SHTR Career Solutions, INDELTA

All correspondence relating to the conference and papers should be sent to:

Dr. Ajay Kr. Singh
Secretary General, Conference Secretariat
C/o Delhi School of Professional Studies and Research
D – 31 & 27, New Delhi South Extension (NDSE), Part – I
New Delhi – 110049, India
Phone: 91-11-4654275/76, Tele-Fax: 91-11-4654277; 7142627
E-mail: aks@shtr.org, drajayksingh@hotmail.com, 4ic@drajayksingh.com
Please visit our web site at: http://www.shtr.org/4ic.html