

**A STUDY OF SELECT ISSUES IN
INFORMATION SECURITY MANAGEMENT
IN INDIAN ORGANIZATIONS**

MUKTESH CHANDER



**DEPARTMENT OF MANAGEMENT STUDIES
INDIAN INSTITUTE OF TECHNOLOGY DELHI
NOVEMBER 2013**

© Indian Institute of Technology Delhi (IITD), New Delhi, 2013

**A STUDY OF SELECT ISSUES IN
INFORMATION SECURITY MANAGEMENT
IN INDIAN ORGANIZATIONS**

by

Muktesh Chander
Department of Management Studies

Submitted
in fulfillment of the requirements of the degree of

DOCTOR OF PHILOSOPHY

to the



**INDIAN INSTITUTE OF TECHNOLOGY DELHI
HAUZ KHAS, NEW DELHI – 110016 (INDIA)
NOVEMBER 2013**

CERTIFICATE

The Thesis entitled “**A Study of Select Issues in Information Security Management in Indian Organizations**” being submitted by **Mr. Muktesh Chander** to the Indian Institute of Technology New Delhi, for the award of degree of **Doctor of Philosophy (Ph.D.)**, is a record of bonafide research work carried out by him. He has worked under our guidance and supervision and has fulfilled the requirements for the submission of this thesis, which has attained the requisite standard required for a Ph.D. degree of this institute. The results presented in this thesis have not been submitted elsewhere for the award of any degree or diploma.

(Dr. Sudhir K. Jain)
Professor
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi-110016
INDIA

(Dr. Ravi Shankar)
Professor
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi-110016
INDIA

ACKNOWLEDGEMENTS

It is my proud privilege to have worked with Professor Sudhir K. Jain and Professor Ravi Shankar. I am highly indebted to them for their initiation, encouragement, continuous motivation and guidance at each stage of this study. I would specially like to thank Dr. Gulshan Rai, Director General, Indian Computer Emergency Response Team (CERT-In), Dr. Kamlesh Bajaj, Chief Executive Officer, Data Security Council of India, Sh. Subimal Bhattacharya and Advocate Pavan Duggal who gave most valuable inputs from time to time. My sincere thanks are also due to Sh. Ranjit Narain IPS (Retd.), the then Special Commissioner of Delhi Police, who motivated me to pursue this study. Sh. Ashok Bhatnagar, GM (CIT), BHEL and Mr. Pankaj Goel, Chief Executive Officer, CresTech Software Systems Pvt. Ltd. also need a special mention for giving me ample time for interviews and access to various documents related to implementation of information security measures in their organizations. I am also grateful to Sh. P. V. Kumar, Ex-Chairman, National Technical Research Organization, Government of India, under whom I worked towards the goal of protection of National Critical Information Infrastructure in India.

I would fail in my duty if I do not place my appreciation for my wife Sunita and my sons Ashish and Varun, who sacrificed and gave away their share of my time for this study.

Date: 22 November 2013

(Muktesh Chander)

ABSTRACT

Information and Communication Technology (ICT) has revolutionized the way we deal with information, do business, communicate and interact with others. It has impacted every sphere of human activity. It is a great tool for organizations for improving competitiveness, quality, productivity and efficiency. In order to reap the full benefits of ICT, organizations need to secure their ICT assets. Cyber security breaches, in ICT dependent organizations, have set alarm bells ringing, forcing them to initiate information security measures. As the Indian organizations are adopting ICT for productivity and output growth, they are also witnessing its dark side. Several Indian organizations have become victim of information security breach incidents in the last few years. Information Security Management has emerged as a multi-disciplinary paradigm attracting the attention of top management of organizations which have valuable information assets, yet it has not received adequate attention in Indian organizations.

This research is aimed at examining various issues related to information security management in different types of Indian organizations. For this purpose, current status of information security management in select Indian organizations has been studied through a questionnaire-based survey to gain insight into various issues related to information security management. Seven hypotheses, related to information security management issues, in Indian organizations, have been developed and tested. A detailed study of global information security environment has been carried out with reference to various international standards and efforts made by international bodies towards information security. International benchmarking has been carried out to find the gaps in information security measures being taken by Indian organizations, as compared to those in USA and

European Union. Two case studies have been developed about information security management practices in two different types of Indian organizations. These case studies have been discussed and analyzed using SAP-LAP (Situation, Actor, Process – Learning, Action, Performance) methodology. Important parameters of information security management for Indian organizations have also been identified and the hierarchical relationships among them have been established.

Information security is a multi-faceted subject and there is a great need to carry out independent research in the related aspects such as, technological issues, cultural issues, manpower and training issues, legal issues, human issues, organizational information security measures, etc. The scope of the present research is limited only to the information security ecosystem prevailing in Indian organizations. The focus of this research is mainly on macro issues like information security policy, training and awareness, organizational information security measures, etc. The research deals with variables related to enablers of information security. Many of the technological issues, economic issues, information security metrics, etc. are beyond the scope of this research. Most of the organizations selected for the study are in the area of Delhi and National Capital Region (NCR) of India.

The study has come out with several findings which are of immense importance for Indian organizations. It has identified the factors, which influence the status of information security. The study has identified the key parameters which affect and significantly influence the status of information security of an organization. It has also identified the large gaps which Indian organizations need to fill to enhance information security. It has also identified the key drivers of information security on which Indian

organizations need to concentrate for effective improvement in information security. The study findings indicate that Indian organizations in IT, BPO and Telecom sectors are the worst affected by information security breach incidents even though they are better than the organizations in other sectors in implementing organizational information security, information security policy, information security awareness & training and use of various security tools and technologies. Indian SMEs in particular, need to take steps to enhance their information security measures more than large organizations. The study has also suggested several measures to be taken by stakeholders such as individual organizations, government and academia, to improve the information security environment.

TABLE OF CONTENTS

	Page No.
Certificate	i
Acknowledgements	ii
Abstract	iii
Table of Contents	vi
List of Figures	xi
List of Tables	xiii
List of Appendices	xvi
Abbreviations	xvii
Chapter 1	
Introduction	1
1.1 Introduction	1
1.2 Major Issues of Information Security Management for Organizations	3
1.3 Major Information Security Breaches	3
1.4 Major Issues of Information Security at Global Level	7
1.5 Scope of Research	8
1.6 Research Questions	9
1.7 Objectives of the Present Research	9
1.8 Research Methodology	10
1.9 Chapterization Scheme	12
1.10 Concluding Remarks	13
Chapter 2	
Literature Review	14
2.1 Organization of Literature Review	14

2.2	Digital Society	16
2.3	Information and Communication Technology Revolution	18
2.4	ICT Revolution in India	19
2.5	E-Commerce in India	22
2.6	Software Export and BPO Industry in India	22
2.7	National E-Governance Plan	23
2.8	Global Information Security Environment	26
2.9	Indian Information Security Scenario	27
2.10	Cyber Crime	29
2.11	Classification of Cyber Crimes	33
2.12	Information Security	48
2.13	Evolution of Information Security	50
2.14	Information Security Principles	53
2.15	Information Security Components	54
2.16	Need for Information Security	57
2.17	Technological Solutions for Information Security	58
2.18	Information Security Management	60
2.19	Organizational Information Security Measures	64
2.20	Top Management Commitment	65
2.21	Identification and Classification of Information Assets of Organization	66
2.22	Information Security Policy	66
2.23	Effectiveness of Information Security Policy	68
2.24	Providing Organizational Structure and Resources for Information Security Functions	70
2.25	Physical and Environmental Security of Organization	70
2.26	Human Aspects of Information Security	71
2.27	Insider Threat	73
2.28	Information Security Awareness and Training	74
2.29	Motivation	79
2.30	Reward and Punishment	80
2.31	Developing Information Security Culture	81

2.32	Information Security Audit, Testing and Certification	82
2.33	Compliance to Legal and Regulatory Provisions	82
2.34	Incident Management, Business Continuity Planning (BCP) and Disaster Recovery (DR)	83
2.35	Gaps in Literature	84
2.36	Motivation for Research	87
2.37	Concluding Remarks	87

Chapter 3

A General Study of Global Scenario of Information Security Management	89
3.1 Efforts by UN and other International Bodies	89
3.2 International Standards	93
3.3 Concluding Remarks	98

Chapter 4

Design of Questionnaire, Pilot Study and Sample Profile	99
4.1 Pilot Testing and Questionnaire Administration	100
4.2 Survey Responses and Respondents' Profile	100
4.3 Reliability of Questionnaire Survey	102
4.4 Observations from the Survey	103
4.5 Concluding Remarks	112

Chapter 5

Hypothesis Development and Testing	114
5.1 Difference in Information Security Management in Various Sectors	114
5.2 Difference in Information Security Management among the Organizations with Foreign Clients and without Foreign Clients	122
5.3 Difference in Information Security Management due to Origin	126

5.4	Parameters which significantly affect Information Security	130
5.5	Difference in use of Security Tools/Technologies of Information Security in various Industry Sectors	134
5.6	Difference in Information Security Management among the Organizations of Different Sizes	136
5.7	Concluding Remarks	144
Chapter 6		
International Benchmarking and Gap Analysis		149
6.1	Benchmarking Study	150
6.2	Profile of Experts and Approach to Data Collection	152
6.3	Major Findings	156
6.4	Concluding Remarks	165
Chapter 7		
Interpretive Structural Modelling of Enablers of Information Security Management in an Organization		168
7.1	Identification of Information Security Enablers	168
7.2	Interpretive Structural Modelling (ISM)	169
7.3	MICMAC Analysis	182
7.4	Concluding Remarks	183
Chapter 8		
Case Study Development and Analysis		186
8.1	Case Study 1	186
8.2	Case Study 2	198
8.3	Concluding Remarks	203

Chapter 9

Discussion and Conclusions	204
9.1 Key Findings	205
9.2 Implications of the Research for Academicians, Industry and Government	207
9.3 Limitations of the Study	211
9.4 Scope for Future Research	211
9.5 Discussion and Conclusions	211
References	213

Appendices

No.	Title	Page No.
A1	National Telecom Policy of India, 2012	243
A2	National Cyber Security Policy of India, 2013	245
A3	Controls and Guidelines for Protection of National Critical Information Infrastructure of India	261
A4	Questionnaire for Survey	263
A5	Questionnaire Survey for Benchmark Study	269
A6	Brief Curriculum Vitae	271