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

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

Chapter 9

Appendices