INFORMATION SECURITY MANAGEMENT MATURITY:

A STUDY OF SELECT ORGANIZATIONS

ABHISHEK NARAIN SINGH

DEPARTMENT OF MANAGEMENT STUDIES

INDIAN INSTITUTE OF TECHNOLOGY DELHI

MARCH, 2014

INFORMATION SECURITY MANAGEMENT MATURITY:

A STUDY OF SELECT ORGANIZATIONS

By

ABHISHEK NARAIN SINGH

Department of Management Studies

Submitted

In fulfillment of the requirements of the degree of

Doctor of Philosophy

to the

Indian Institute of Technology Delhi

March, 2014

CERTIFICATE

This is to certify that the thesis entitled "Information Security Management Maturity: A Study of Select Organizations" being submitted by *Abhishek Narain Singh* to the Department of Management Studies, Indian Institute of Technology Delhi for the award of the 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 fulfilled the requirements for the submission of the thesis, which has attained the standard required for a Ph.D. degree of the institute. The results presented in this thesis have not been submitted elsewhere for the award of any degree or diploma.

(Prof. M. P. Gupta)

Research Supervisor
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi – 110016, India

(Dr. Amitabh Ojha)

Research Supervisor
Research Design and Standards Organization
Ministry of Railway, Government of India
Lucknow – 226011, India

ACKNOWLEDGEMENT

I express my deepest gratitude to my guides, Prof. M. P. Gupta and Dr. Amitabh Ojha, whose continuous support and guidance on every step helped me understand the research problem, issues, and finally in writing the thesis. I am indebted for their personal support and professional guidance in the area of data analysis, its interpretation, and presentation of the facts in a structured format. They also provided me a valuable learning environment that helped in evolving and familiarizing the information security management concepts for this research study.

I am grateful to Prof. Sushil for his rich scholarly inputs that facilitated my research work. I also sincerely thank to Prof. S. K. Gupta and Prof. S. K. Jain for their support and encouragement while pursuing my research work. I am very much thankful to the academicians, reviewers and editors for their valuable comments on my papers submitted for conferences/journal publications.

I am very much thankful to the Deutscher Akademischer Austausch Dienst (German Academic Exchange Service) for providing me the opportunity and financial support to work in the Institute for Information, Organization, and Management - Munich School of Management at Ludwig-Maximilians-University Munich in Germany as a visiting scholar. I am grateful to Prof. Dr. Dres. h.c. Arnold Picot and Prof. Dr. Johann Kranz, with whom I worked during my stay in Germany, for their valuable suggestions and inputs to my research study.

It will be unfair to forget my fellow research colleagues including Dr. M. M. Chaturvedi, Dr. Sreejith, Mr. Amit Srivastava, Mr. Krishnendu Shaw, Ms. Priyanka Jaiswal, Mr. Sumant Biswas,

and Felix Haeussinger who provided their personal support and valuable inputs throughout my doctoral work. I am also grateful to Mr. Vijay Devnath and Mr. Vineet Sehgal who were very kind and supported me a lot on the task of data collection. I am thankful to the respondents to my study, for their time and support for this study. I also thank the office staff of Department of Management Studies for their assistance and cooperation.

Nevertheless, for the grace of God and good wishes of my family members and friends, it would not have been possible to complete the work.

New Delhi (Abhishek Narain Singh)

Abstract

In this research, study of information security practices of select organizations has been carried out with the aim to derive useful lessons. This is relevant as in present era of borderless and highly connected modern organizations, the use of IT/ICT mediums for conducting various business processes have become inevitable. The organizations have become, and becoming, more and more dependent on their information systems day-by-day. Depending upon the nature of work, it is nearly impossible for many organizations to conduct day-to-day operations without proper functioning of their information systems. In such a scenario, securing business information and information assets from unauthorized access, loss, and misuse have become a challenge for organizations.

In past, managing information security in organizations has largely been a technical challenge. Therefore, the focus of the discipline has been more on the technological aspects of information security. With maturity of the information security literature, the discipline has evolved over the period in many waves, such as, management, organizational and institutional. The evolution has witnessed the introduction of various management, human, organizational, behavioral, legal, and other aspects along with the technical side of the discipline. In the course of literature review for the present research study, multiple dimensions of information security highlighted by previous researchers were studied, and various information security management (ISM) frameworks were examined. As highlighted by scholars, there is a gap of a comprehensive ISM framework which focuses on the management aspects of information security in organizations. Taken this in account, this research applies mixed method approach to investigate various management factors related to information security in organizations across all levels.

In the exploratory phase of the research, comprehensive literature review on the subject was done. Keyword analysis was applied to identify various dimensions/factors of organizational ISM. To supplement the findings of literature review, participation in various conferences, workshops and seminars on the subject was made. This helped to understand and explore key challenges of organizational ISM and current issues in this field. In addition, views of experts

from industry, academia and government were solicited to confirm the organizational ISM factors and various linkages among them. This enabled to develop an empirical organizational ISM framework for the study.

The framework presents ISM as a management phenomenon for organizations. In a holistic approach, framework integrates ISM activities from all the three levels; strategic, tactical and operational in an organization. The Conceptual framework, in the form of an input-process-output model, considers ISM as a dynamic, repeatable and self-improvement exercise for organizations. Input dimension consist ten ISM factors from various strategic, tactical, operational and performance level factors of organizational ISM. The process dimension refers Plan-Do-Check-Act (PDCA) cycle that shows ISM as a continuous and self-improvement exercise for organizations. However, output is measured in terms of organizational ISM maturity.

As the extant literature on ISM suggests, information security maturity is the current status of ISM practices of an organization. Scholars draw attention towards a gap for a mechanism to measure the information security practices, and thus the evaluation of ISM maturity of organizations. To fulfill this gap, the present study develops an ISM maturity assessment instrument with the help of literature review and experts' opinion. The instrument evaluates the current ISM practices of organizations on a five level maturity scale.

Next, in the empirical phase of the research, a questionnaire based survey was conducted for respondents across the hierarchy and functions in organizations from multiple industries (IT, telecommunication, banking, transportation and others) to test the empirical organizational ISM framework. A questionnaire tool was developed, pilot tested and checked for its validity and reliability. Various statistical tests were performed on the received responses to examine and validate the linkages among various organizational ISM factors, as identified from the exploratory study. Further, suitable statistical analyses (such as correlation, step-wise linear regression, structural equation modeling, etc.) were conducted to verify the structural relationships among various strategic, tactical, operational, and performance factors of organizational ISM.

In the third phase of the research, six case studies were conducted using qualitative research approach to examine the ISM practices of select organizations and to access their current ISM maturity levels. In a multi case study design, six medium and large size organizations from IT-development and services, telecommunication infrastructure services, and, IT and business consulting industries were selected. Out of six, three organizations are from India and other three are from Germany. In total 42 semi-structured interviews were conducted from employees across the hierarchy in organizations. An interview questionnaire template was used for this purpose. All the interviews were conducted face-to-face, in the regular settings of respondents and were audio recorded. Each interview lasted approximately 45 to 50 minutes and their transcript was made for further analysis of the interview data. Key observations from the interviews were presented using descriptive analysis methodology. Further, SAP-LAP (Situation, Actor, Process – Learning, Action, Performance) method of inquiry was used to analyze the cases. In addition to this, ISM maturity evaluation of the case organizations was done using the ISM maturity assessment instrument developed for the research study.

Finally, a synthesis exercise was done to derive the learnings from various phases of the research. Implications are derived from the findings of exploratory, empirical and case studies for practitioners as well as for research. Limited response rate for questionnaire based survey and case studies from few select industries are the limitations of present research study. Key contributions of the research include the proposed organizational ISM framework and the ISM maturity assessment instrument for organizations. This study also opens avenues for future research as; the framework suggested in this research can be applied and tested in varying contexts (e.g. industries, sectors, etc.), and further research can be conducted focusing separately on various strategic, tactical, operational and performance factors of organizational ISM.

Table of Contents