Analyses of issues of information security in Indian context

Article *in* Transforming Government People Process and Policy · August 2014

DOI: 10.1108/TG-07-2013-0019

CITATIONS
10

READS
2,225

4 authors:

Manmohan Chaturvedi
Indian Institute of Technology Delhi
5 PUBLICATIONS **19** CITATIONS
SEE PROFILE

Abhishek Narain Singh
Institute of Management Technology Nagpur
8 PUBLICATIONS **233** CITATIONS
SEE PROFILE

MP Gupta
Indian Institute of Technology Delhi
132 PUBLICATIONS **3,064** CITATIONS
SEE PROFILE

Jaijit Bhattacharya
Indian Institute of Technology Delhi
33 PUBLICATIONS **255** CITATIONS
SEE PROFILE

Transforming Government: People, Process and Policy

Analyses of issues of information security in Indian context

Manmohan Chaturvedi Abhishek Narain Singh Manmohan Prasad Gupta Jaijit Bhattacharya

Received 3 July 2013
Revised 2 January 2014
4 February 2014
19 March 2014
Accepted 26 March 2014

Analyses of issues of information security in Indian context

Manmohan Chaturvedi
Ansal University, Gurgaon, India, and
Abhishek Narain Singh, Manmohan Prasad Gupta and Jaijit Bhattacharya
IIT Delhi, New Delhi, India

Abstract

Purpose – The purpose of this paper is to attempt to fill the need to identify critical information security issues at national level, both technical and social in the Indian context, and create a framework of these issues to provide interesting managerial insights about their hierarchy. Current literature advocates relevance of both technical and social issues in a potential framework to address national and organizational information security concerns. Such a framework can guide users in developing insight for strategy in the maize of important information security issues and their intricate interdependency.

Design/methodology/approach – Delphi methodology is used to identify a set of topical issues with help from members of a cyber security group. These issues are further analyzed using Interpretive Structural Modeling (ISM) to impose order and direction to the complex relationships among them.

Findings – The analysis using ISM creates a framework of these issues and provides interesting managerial insights about their hierarchy. These insights are used to recommend prioritized action for information security at national and organizational levels.

Research limitations/implications – The highlight of this research is ingenious deployment of two idea engineering methods in developing interpretable structural model of 25 information security issues. This model provides valuable insights and can guide the policy formulation. This is the key contribution of this paper. It needs hardly any emphasis on the need for continuous search of all technical and social issues and formulating policies and programs using experts" judgment in a rigorous manner. Subsequent research may scale up to the global level for extension and validation by empanelling Delphi experts from nations belonging to different regions. Time-variant analysis can be attempted with the help of System Dynamics Modeling using causal-loop diagrams to account for the supportive and inhibiting influences of various issues. This approach has the potential to generate more realistic insights that can inform policy formulation.

Practical implications – It brings about key information security issues connected with its various facets, viz. national/organizational level initiatives, supportive processes, capabilities and objectives. These issues, identified by Indian experts in the Indian context, offer a method that one could apply in other national contexts and see whether substantial differences occur, and how other experts prioritize these issues. The analysis of social issues along with technical issues using the ISM tool provides us insights that are considered applicable to a larger context than India. The policy and program formulations in other nations can benefit from the insights generated by this research. The fast-paced proliferation of technology and its resultant vulnerabilities have given birth to an underground economy of malware trading by criminals, terrorists and hostile nation states. Secure cyber space for legitimate use by the globalized world can only be achieved by international cooperation.

Social implications – A "digital divide" in cyber defense cannot be afforded. As explained earlier, cyber security is a challenge for both developed and developing nations. Prioritization of resources in a

Transforming Government: People, Process and Policy
Vol. 8 No. 3, 2014
pp. 374-397

1750-6166
DOI 10.1108/TG-07-2013-0019

sequence suggested by ISM analysis would help face the challenge of cyber security better. The methodology suggested in this paper would ensure adequate response to cyber threats and eliminate knee-jerk reaction.

Originality/value – This research emphasizes identification of hierarchical relationship among the identified topical issues of information security rather than using them as a flat checklist. It helps us segregate the end objectives from root issues and highlights the necessity of addressing these root issues to achieve those objectives.

Keywords Information security, Delphi, Hierarchical analysis, Interpretive structural modeling (ISM)

Paper type Research paper

1. Introduction

The transformation of "industrial age economy" to "information age economy" has resulted in the creation of information infrastructures in almost all the nations of the world (Nicholson *et al.*, 2012). The economy and convenience in using this infrastructure in an era of globalization has been the prime motivator. Unfortunately, inimical interests have also grown alongside to exploit the vulnerabilities of this infrastructure to act as a damper to unrestricted use of these information highways (Choo, 2011; Martin and Rice, 2011).

The phenomenon of targeting the emerging societal infrastructures by the criminals is not new. Highway robberies, sea piracy and hijacking of civil aircrafts have been the known challenges to mankind on its way to an interconnected world. International cooperation combined with regulatory and legal frameworks has helped in deterring criminals and terrorists. Information highways, because of their international reach and economical mode of communication of data, voice and video, are attractive to both law-abiding citizens and criminals, as these new media channels can be used as a medium for propaganda such as publishing doctrines, promoting extremism activities, recruitment and training of potential terrorists and transferring information (Choo, 2011). International efforts to secure the information highway have yielded results. However, with increasing stakes and evolving technology, cyber criminals have graduated to professional status using sophisticated automated tools. Therefore, the balance is not always in favor of genuine users of this highway. It is going to be a long drawn out race for supremacy between legitimate users and the criminals in the cyber domain, with stakes becoming higher with increased adoption of online governance and commerce (Choo, 2011; Martin and Rice, 2011).

National security planners have begun to look beyond reactive, tactical cyber defense to proactive, strategic cyber defense, which may include international military deterrence. Real-world examples suggest that cyber warfare will play lead role in future international conflicts (Geers, 2010a). The Stuxnet, Duqu and Flame worms, as reported in media, target industrial control systems and herald the beginning of workable cyber attack approaches against critical industrial infrastructures of a nation.

Recently documents released by the US whistleblower Edward Snowden suggest that the US National Security Agency may have accessed computers within installations of other countries in Washington and mission at the United Nations in New York as part of their effort to mine available electronic data (The Guardian, 2013). The row arising of this has rattled global politics. World leaders are beginning to look beyond temporary fixes to the challenge of securing the Internet.

Not all information is in computers – so cyber security is just a subset of the larger area of information security. Cyber security is the use of various technologies and processes to protect networks, computers, programs and data from attack, damage or unauthorized access. Information security, on the other hand, involves protecting information from unauthorized access, use, disruption, modification or destruction, regardless of whether the information is stored electronically or physically. For an individual, information security has a significant effect on privacy, and organizations now treat information security as part of serious business issues and started establishing cross-organizational teams to discuss and manage these issues (Westby, 2010). With increasing incidences, and serious consequences, information technology (IT) security and risk expertise are now recognized as important skills at higher-level positions. In the past decade, information security has evolved from earlier technology focus to management focus both at organizational (Anderson and Choobineh, 2008) and national levels (Cyberspace Policy Review, 2009). The social dimension and necessity to have socio-technical frameworks at the national level are being explored in recent literature (Shin, 2010). The trend to analyze information security from systems perspective seems to be gaining currency (Chang and Wang, 2011). However, a system perspective could as well be at an enterprise level, and it does not necessarily mean a national-level macro-perspective.

1.2 Motivation for research

A macro-perspective is easier to build if we have clarity about multiple factors that describes the prevailing environment of information security threat. Further, knowledge of their interplays enhances our ability to derive a good policy and prepare effective action plan. Motivation of this research is drawn from the current literature that emphasizes on a holistic approach in addressing national and organizational information security factoring both technical and social issues. There is a clear need of a framework that can guide users in developing insight for strategy in the maize of important information security issues and their intricate interdependencies. An insight into their causal relationships is expected to help policymakers, both in government and private sectors, to prioritize them realistically. Therefore, this paper, attempts to identify macro-level key issues of information security at the national level and establish a hierarchical relationship among them.

Rest of the paper flows in the following manner: Section 2 reviews the literature followed by Section 3 outlining the design of the research undertaken. Section 4 reports results of the research. Section 5 is the discussion of results and the managerial insights. Policy implications, practical application of these insights to international context from the Indian context, the future research implications of this paper and implications for practice are also highlighted in this section. Section 6 provides concluding remarks for the paper.

2. Literature review

How can we investigate the underlying trends in information security? What could possibly be surrogate indicators of important information security issues? The real-world incidents and developments connected with information security invite attention of researchers to analyze the issues and suggest possible remedies.

The management's concern with securing the information infrastructure from insider threat (Catrantzos, 2010; Colwill, 2009) is a departure from exclusively technology focus in the past. The pivotal role of awareness and training in securing cyber space has finally been conceded (McCrohan *et al.*, 2010). Necessity of supportive legal frameworks (Gerber and von Solms, 2008) has been clearly articulated.

In a recent paper, Polónia and de Sá-Soares (2013) have identified 26 key issues in information security management and prioritized them. Having an enterprise-level focus, their study has limited purpose to serve, as national and international issues are not the scope of their work. The cyber domain does not respect geographical borders, and therefore, any holistic framework for ensuring information security at the enterprise level cannot ignore the eco-system provided by the national-level governance and international treaties that shape responses to cyber crime, cyber terrorism and also cyber warfare.

The Internet is a reality of our life and adapting to its dynamics (Jung *et al.*, 2010) is being attempted by all enterprises (Westby, 2010, CyLab Report, 2010). As most of the information infrastructure is owned and operated by the private sector while its security is a national-level issue, the role of public–private partnership (Navare and Gemikonakli, 2010) and search for novel approaches for law enforcement in cyber space describe the current landscape (Oliver, 2009).

Moving beyond the enterprise level, the information security policies are being framed at national levels and articulated in public domain (DHS, 2009; National Cyber Security Policy, 2011). National security is being linked with cyber space (National Security Threats in Cyberspace, 2009).

The need to have international cooperation for achieving secure cyber space has been recognized and has manifested in formation of various regional and international structures toward this shared objective (Dogrul *et al.*, 2011; Forsyth, 2013; BIC, 2013).

The necessity to measure the impact of policy initiatives towards information security (Goel and ChengalurSmith, 2010; Torres *et al.*, 2009) has been recognized in contemporary literature.

The necessity of a process model factoring security behavior while addressing information security issues is being emphasized (Knapp *et al.*, 2009; Liang and Xue, 2010). One additional area that is driving the information security debate is the evolution of next-generation networks (NGN) that is the substrate on which the future Internet applications would operate (CISCO, 2011).

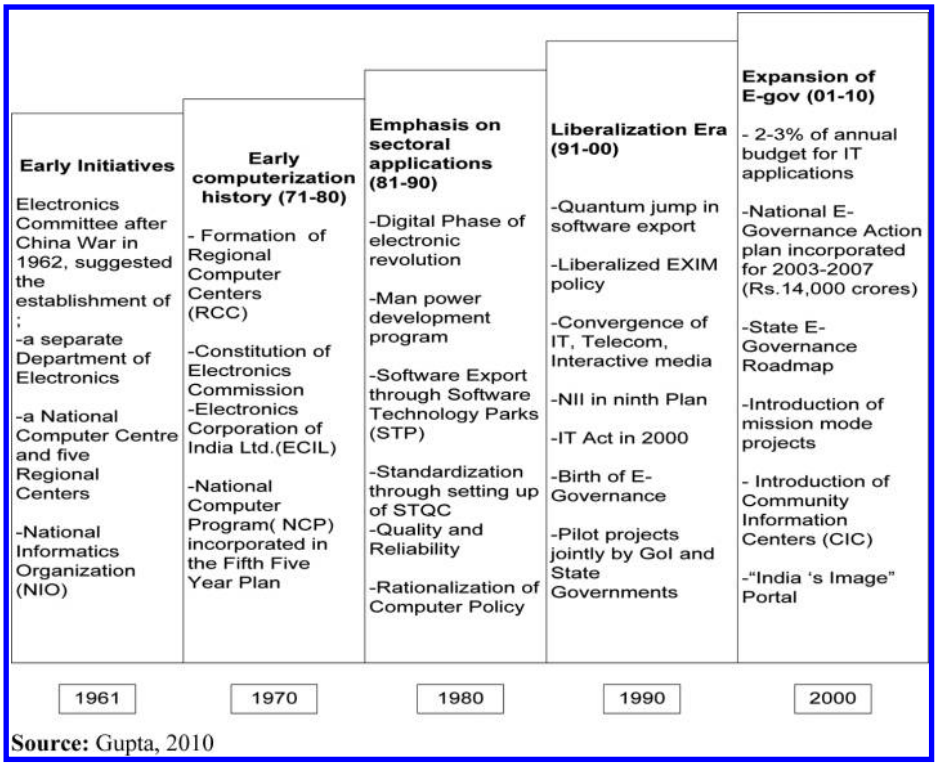
The current literature, therefore, points at a noticeable shift from technical to management perspective, enterprise to national/international level and need to measure the impact of various initiatives through a holistic framework.

Thus, there is a case for identifying a more holistic framework of the issues going beyond enterprise level and factoring in the challenges created by futuristic NGNs being rolled out at an increasing rate.

As this research has India as context, we need to analyze the evolution of IT applications in the government in India and thus be able to discern the key issues that could describe their security concerns. To support this critical objective, following paragraphs attempt to describe the evolution of IT applications in India over the past five decades. We would be able to derive useful managerial insights from the findings of this research with this context in place.

Gupta (2010) has tracked the evolution of IT applications in the government starting from 1960s when the inadequacy of the existing telecommunication infrastructure in India during her war with China in 1962 triggered the process of revamping this sector. Figure 1 adapted from this paper depicts very succinctly the decade-wise evolution from simple computerization to a national plan on e-Governance in India.

The enactment of IT Act 2000 by the Indian Parliament was the most significant step that allowed electronic records, digital signatures and a notification in electronic gazette to be legally recognized. Further, to give effect to these provisions, appropriate amendments have been made in the Indian Penal Code-1860, the Indian Evidence Act-1872, the Bankers' Books Evidence Act-1891 and the Reserve Bank of India Act-1934. These amendments have made these statutes compatible with the "e-justice system". Despite the IT Act in place, the recent few years have seen a rise in hacking, Web site defacement, breach of privacy and data theft. The business process outsourcing (BPO) industry was much affected by data theft reported in 2004-2005, putting a question mark on the credibility of the IT sector. In view of this, The IT Act 2000 has been substantially amended to deal with new forms of cyber crimes like publicizing sexually explicit material in electronic form, video terrorism and breach of confidentiality and leakage of data by intermediary and e-commerce frauds through the IT Amendment Act 2008 which was passed by the two houses of the Indian Parliament on December 23 and 24, 2008. It got the Presidential assent on February 5, 2009 and was



Source: Gupta, 2010

Figure 1.
Transition of Indian e-Governance systems over the decades

notified for effectiveness on October 27, 2009. The rules of important sections under the Act were also notified and enforced. The formulation of rules for additional sections under the Act is in the process. Following the November 2008 terrorist attacks in Mumbai and with an expanding Maoist insurgency, the Indian Government through new amendments in the IT Act, 2011, has armed itself with powers to "switch off" or kill the Internet during times of national emergencies, becoming one of the first few countries to assume such far-reaching authority. There have been public debates in India after details of the "GhostNet", a cyber espionage network believed to be operating from China, were revealed by a Canadian research group in March 2009 (Bajaj, 2010). It has brought out another report named "Shadows in the Cloud" that describes an ecosystem of cyber espionage that has been built on "GhostNet" infrastructure and presents emerging national security challenges of the nations in cyber space (IWM-SF, 2010). The Indian Government has initiated, in the recent past, certain strategic measures to meet the growing threat in cyber space.

According to a report in ORF Cyber Monitor (ORF, 2013), the Indian Government's Cyber Security Policy – unveiled on July 2, 2013 – will have a wide reach, with a National Nodal Agency being set up which will cover and coordinate security for all strategic, military, government and business assets. This is distinctive, as so far, national security regimes have been divided among the Ministry of Defense (for securing India"s borders) and the Ministry of Home Affairs (for national and internal security across States).

India cyber security Joint Working Group was set up under the chairpersonship of Deputy National Security Advisor in October 2012 for engaging the private sector in a public private partnership (PPP) for strengthening the cyber security architecture in the country (The Hindu, 2013).

Gupta *et al.* (2004) have reported important security factors based on a survey carried out in India on government organizations and their threat perception. Interactions with experts helped in identifying following ten important factors:

(1) access to data/systems by outsiders (hackers);
(2) intentional/accidental destruction of data by employees;
(3) viruses, bombs, worms, etc.;
(4) inadequate or non-existent logon procedures;
(5) loss due to inadequate backups or log files;
(6) inadequate administrative mechanisms (policies, procedures, etc);
(7) weak/ineffective or inadequate physical control;
(8) uncontrolled user privileges (read and/or update access);
(9) natural disaster: fire, loss of power, flood, etc.; and
(10) lack of security consciousness amongst employees).

2.1 Research gap

These factors, except the last, are mainly technology and procedure focused. However, as information security is a rapidly evolving discipline, it is important to include more topical issues and merge others still relevant to refresh the picture of the cyber security landscape with current realities. Evidence from the above literature review suggests that we include management, social and legal dimensions while seeking comprehensive

solutions. Increasingly globalized world with blurring borders for information flow emphasizes international outlook while attempting to secure our cyber space.

3. Design of research

3.1 The research question

With the above motivation, we attempt to bridge the research gap by asking the following three research questions:

RQ1. What are current issues driving information security in the Indian context?

RQ2. What relationship exists among these identified issues?

RQ3. Could we derive a framework using these relationships discerned through our research?

To have an answer to these research questions, the present study set the following three objectives driving the subsequent research:

(1) identification of both technology and social issues of information security in the Indian context;

(2) establish direct and indirect relationships amongst these issues; and

(3) using these relationships among identified issues evolve a structure to guide the information security program formulation in a national context

3.2 Research methodology

Choice of a research method is governed by research questions and objectives set therein. Because the present study is heavily dependent on expert opinion, their participation in idea generating exercise is central to the entire research effort (Figure 2). Information security is a subject where obtaining a trustworthy opinion from experts in an open idea sharing or brainstorming session is prone to biases or conflicts. It is, hence, logical to rely on proven Delphi methodology for this research where not only we confront many issues but also complexity of their interplay is beyond one person's

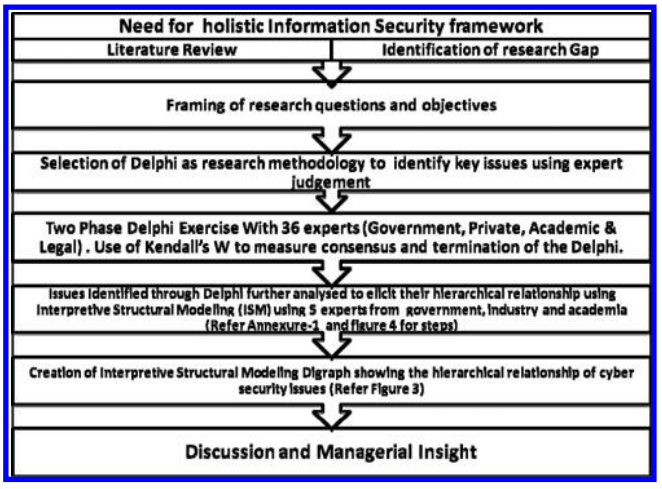


Figure 2.
Research flow diagram

comprehension. The Delphi technique is chosen, as it ensures anonymity of the experts and can be implemented from any location, so economical and logistically convenient (Dalkey and Helmer, 1963; Gordon and Helmer, 1964; Linstone and Turoff, 1975; Turoff, 1970; Parente *et al.*, 1984; Rowe and Wright, 1999).

It allows capitalizing on experts' wisdom (practicing professionals and academics) about issues connected with information security at the national level and capture diverse and rich background data in the form of expert comments besides quantitative Likert-scale data. Internet has been helpful in getting responses in a relatively short period of time with convenience of Delphi members. Delphi group here was constituted by inviting the members of an information security forum that seeks to bring together the professionals interested in the area of information security in India. The members are experts from government, industry and academia (Tables I-III). They provided a unique opportunity to the authors to seek consensus views of the representatives of the government, industry and academia. The context of this research was explained to group members, and their comments were requested using the interaction on Internet but maintaining their anonymity. This exercise resulted in 25 issues (Table IV), describing information security ecosystem in India.

It is now necessary to find out the hierarchy of relationship among these 25 issues based on dependency among them. Without an insight into dependency structure of these security issues, they are nothing more than a flat checklist. In complex subjects like information security, with a large number of diverse issues, our ability to reach pragmatic conclusions and communicate to others our rationale for prioritization of issues intuitively is not dependable, and a more structured methodology is required. ISM (Warfield, 1974) is known for developing clarity into large number of issues having a complex relationship. The rigor of ISM provides us with the ability to separate various issues in well-defined levels, much like the process of fractional distillation of petroleum and its products. ISM has been used for policy analysis (Hart and Malone, 1974; Hawthorne and Sage, 1975; Brand *et al.*, 1976; Kawamura and Christakis, 1976) and management research (Mandal and Deshmukh, 1993; You *et al.*, 1994; Jharkharia and Shankar, 2004; Sushil, 2005; Bolaños *et al.*, 2005; Ravi and Shankar, 2005; Kannan and Haq, 2007). Using the aggregation of the expert wisdom, ISM helps to identify the relationship among the issues in a structured manner.

The interplay and dependency of the 25 critical information security issues identified by the Delphi exercise are further analyzed using ISM, so as to articulate the hierarchical relationships among these issues. For the present study, five members of the expert group were identified for collaborative sessions. The experts work in group setting to indicate dependency of related issues. In any complex problem-solving context, certain issues are more important than others, and the prioritization of issues is essential (Figure 2).

Organization	No. of respondents	(%)	Kendall's W
Government	9	25.0	0.285
Private Sector	19	52.8	0.285
Academic	6	16.7	0.352
Legal	2	5.6	0.615
Total	36	100	0.236

Table I. Sector-wise composition of respondents for first phase of Delphi survey

SN	Appointment/profession	Cyber security experience
1	Director	Army, Corps of Signals
2	CCA	Digital certificate systems root certification
3	Professor	Teaches ICT systems to MBA and PhD students
4	Research staff	Working on ICT systems
5	Practicing Advocate	Criminal law
6	Vice President –Information Security (Chief Information Security Officer)	Has a long-standing career of over nine years and comes with diverse knowledge base that includes expertise in information security compliance, data protection and privacy, IT operations and technical project management
7	Scientist "F"	Exposure to PKI practices
8	Vice President–Networks and Systems, Chief Information security officer	More than 15 years experience
9	District Judge	Exposure to the Judicial process
10	CISO	Eight years of work on related areas in Military Intelligence (including training and working on information warfare); two years with Infosys internal Information Security Department; and one year in current assignment
11	Commander	30-year experience in communication and cyber security. Qualified in CISSP,CISA,CEHP and Cyber Law
12	Director	Involved in cyber security issues of Ministry of Defence, Coordinating Crisis management plan of MoD, Interacted with National agencies in formulating policies regarding cyber security
13	General Manager, Financial Crime Prevention	Director, Cyber Security and Compliance, NASSCOM (April 2005-May 2008); GM, Financial Crime Prevention, ICICI Bank (May 2008- till date)
14	Founder	Crime investigation, forensic, offensive attack, training
15	Sc E	10-year experience
16	Founder of a Cyber Security Company	Certified CISA, CISM, ITIL, BS7799, IPR and ERM. Over 10 years in technology and information security. Presently engaged in consulting and advisory services for information security
17	Freelance journalist in Cyber Security Area	8-year experience
18	Researcher	5-year experience
19	Director, Government Affairs	Advising government and CERT
20	Vice President & Head Information Security	11-year experience
21	CEO	Over 15-year experience
22	Partner GRC	9 years. Information security experience: 12 years. Total IT experience: 20 years
23	Technical Officer	Use of ICT systems and their security
24	Lawyer	Legal issues pertaining to Cyber systems
25	AVP–IT and CISO	5-year experience

Table II.
Profiles of the Delphi panel participants

(*continued*)

SN	Appointment/profession	Cyber security experience
26	Information Security Head, India	10-year experience
27	IAF, Research Fellow	3 years
28	CISO	More than 15 years
29	CSO	8-year experience
30	CISO	Over 10-year experience
31	Head of IT Department	More than 20-year experience on IT systems
32	Chief Information Security Officer & Senior Vice President	12-year experience
33	Research Scholar	User of ICT systems
34	Senior Director	Working in Indian Computer Emergency Response Team (CERT-In)
35	CISO	Has handled frauds, hacking, phishing, etc.
36	Professor	Teaching computer science for > 15 years

Table II.

Organization	No. of respondents	(%)
Government	7	29.16
Private sector	12	50.0
Academic	3	12.5
Legal	2	8.33
Total	24	100

Table III. Profiles of respondents for second phase of Delphi survey

A brief about specific steps involved in developing the ISM is presented in Appendix.

4. Results of the research

4.1 Delphi member's empanelment from various stakeholders in the Indian context

A total of 50 potential participants were requested to participate in the research; however, only 36 responded. Effort was made to enroll the members from government institutions that are closely connected with information security policy formulation. The participants from private sector also offered us a wide perspective from IT system security in financial, banking and independent consultancy fields. Sector-wise composition of participants from four sectors, viz. government, private, academic and legal in the first phase is depicted in Table I. These respondents were from senior management levels of the sectors considered (Director and above in government, Vice President and senior managers in private, professors and researchers in academics and senior judge and advocate in legal). Table II provides a view of their roles within the limit of anonymity to be maintained in Delphi process. The Kendall"s W (an indicator for degree of consensus within the group) for the rankings of all identified issues among the participants from four sectors is also indicated in the last column of Table I. The degree of consensus is of the same order, and the higher value in the legal sector is attributed to only two participants in this group. It appears that the ranking of identified issues is not sensitive to the sector of the respondents.

As experienced by other researchers, and reported in literature (Keeney *et al.*, 2001; Sharkey, 2001; Williams and Webb, 1994), the number of respondents for the Delphi panel reduced to 24 (Table III) in second round.

Code no in ISM analysis	Issues identified by members of cyber security group in India as part of this research
1	Top management support at organizational level
2	Legal and regulatory framework to support enforcement agencies
3	Ability to defend against malware
4	Training and security awareness of employees
5	Disaster preparedness
6	Business continuity
7	Adoption of data-driven cyber security investment decisions
8	Hiring of benchmarked security staff
9	Ability to analyze security breaches for corrective action
10	Incident management and response
11	International treaties to address cyber security
12	Risk management in conformity with international standards
13	Managing organizational perception of Info security
14	Vulnerability analysis by IT staff
15	Cyber security governance at national level
16	Software patch management
17	Use of electronic signature and encryption systems
18	Meaningful metrics and measurements
19	Ability for cloud computing and web application security
20	Social sites security issues
21	Psychological factors in insider threats
22	Secure application development
23	Secure adoption of NGNs
24	Information theft issues
25	Use of appropriate information security technology

Table IV.
Top information security issues and factors

4.2 Identified cyber security issues

Through two iterations, the Delphi group was able to generate 38 issues. These issues were rated on five-point Likert scale by the group. The iterations were closed at this stage, as adequate consensus in terms of Kendall's W for the rankings of all identified issues among 24 respondents in the second phase was 0.258. The null hypothesis, that "the experts' ratings in a group are unrelated to each other", was rejected at a 0.05 significance level.

The issues were limited to 25 most important ones based on their mean ranking. Where there was a common mean ranking, the issues considered more important were retained in the final list of 25 issues listed in Table IV. They reflect the increased scope of issues from the earlier identified ten factors by Gupta *et al.* (2004). In Table IV, the issues are listed arbitrarily without any consideration of their mean ranking.

A close look at these factors reveals that no meaningful cyber security is possible without international cooperation and suitable nurturing initiatives by the national governments. This has been endorsed by the experts. Legal and regulatory frameworks are considered essential to empower enforcement agencies. With ubiquitous wireless technologies for networking and challenge in use of Internet for voice communication, the secure adoption of NGNs is also flagged as a security issue. Growing popularity of cloud computing and social sites pose other security challenges. The establishment of meaningful metrics and measurement would ensure data-driven cyber security

investment decisions. In the emerging knowledge economy, the impact of information theft on privacy of privileged organizational information and Intellectual Property Right assumes importance. Use of electronic signature and encryption systems along with secure application development are other issues. Effective cyber security is not possible without addressing psychological factors leading to insider threats, user training and awareness combined with the presence of benchmarked security professionals in key positions. The top management support at the organizational level is considered a catalyst for transforming security stance of an organization.

These25 issues while not exhaustive still provide the basic landscape of the current information security efforts. Building up over this, further research being reported in this paper is based on the assumption that any attempt to measure cyber security should first analyze the interplay and dependency of these issues. This extended and topical set provides us increased scope compared to ten issues – mostly technology and process related identified by the earlier survey. The intervening period between the two surveys also brings to light the changing perspective, viz. a combination of technology and social toward successful implementation of cyber security programs at organizational and national levels. These issues, although identified in the Indian context, are still relevant in the global context because of the global nature of cyber domain and commonality of challenge faced by international community.

Most of the surveyed literature on key issues of information security have an enterprise-level focus. National and international issues seem to have been left out. The anticipated security challenges with adoption of NGNs are also missed out. It is easy to map the enterprise-level issues identified by other recent research with those identified by our research, and it may be construed as an indirect validation of our findings. Thus, our research, while succeeding in eliciting the enterprise-level issues, has gone beyond to map national and international dimensions besides evolving technology trends, e.g. NGNs.

However, the real value of this research is in eliciting a structure among these issues as described in subsequent paragraph using a rigorous methodology, viz. ISM.

4.3 Structuring of critical information security issues using ISM

With the illustrative Indian context in place, we need to view the security of the Indian information infrastructure through the lens of the 25 security issues flagged in Table IV by the Indian security experts. We plan to create a hierarchical relationship among these information security issues using ISM.

ISM is an interactive learning process whereby a set of different, directly and indirectly related elements are structured into a comprehensive systemic model. The model so formed portrays the structure of a complex issue in a carefully designed pattern using graphics as well as words. For complex problem like information security, a number of enablers may be influencing the final goal of effective information security. However, the direct and indirect relationships between the enablers describe the situation far more accurately than individual factors taken in isolation. Therefore, ISM develops insight into collective understanding of these relationships.

The ISM methodology is interpretive, from the fact that the judgment of the group decides whether and how the variables are related. On the basis of relationships, an overall structure is extracted from the complex set of variables. It is a modeling technique in which the specific relationships of the variables and the overall structure of

the system under consideration are portrayed in a digraph model. ISM is primarily intended as a group learning process.

Expert opinion for ISM may be collected with the help of any group technique (Delphi, brainstorming, Nominal Group Technique, etc.) in developing the contextual relationship among the variables. This paper is using as an input to ISM the critical information security issues identified by the members of an Indian cyber security group.

The ISM analysis provides us with a hierarchy of security issues in the form of a digraph depicting dependency relationships as shown in Figure 3.

As can be seen, the national-level policy and initiatives (showed as level V issues in Figure 3), viz. cyber security governance at the national level (15), international treaties to address cyber security (11) and legal and regulatory frameworks to support enforcement agencies (2) drive the organizations dependent on their information infrastructures for day-to-day functioning.

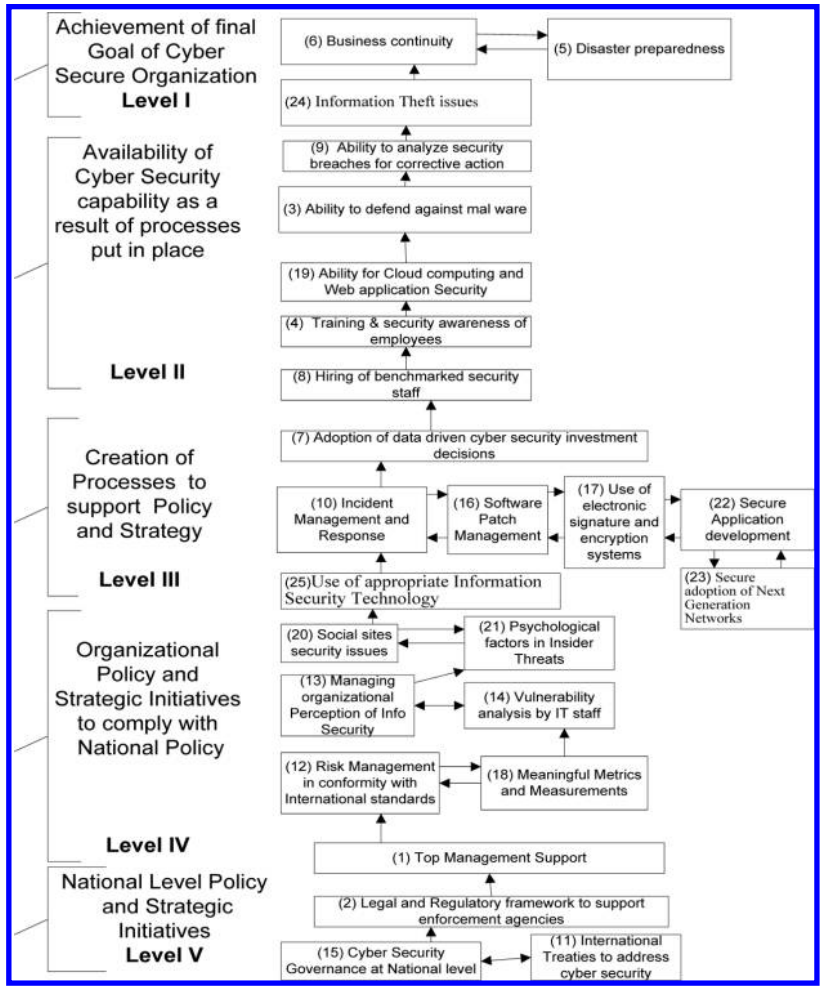


Figure 3.
ISM digraph showing the hierarchical relationship of cyber security issues

The organizational initiatives (showed as level IV issues in Figure 3) by way of top management support (1), risk management in conformity with international standards (12), meaningful metrics and measurements (18), vulnerability analysis by IT staff (14), managing organizational perception of information security (13), addressing psychological factors in insider threats (21), social sites security issues (20) and finally use of appropriate information security technology (25) become the basis for sustainable processes.

The creation of processes (showed as level III issues in Figure 3) like, ensuring secure adoption of NGNs (23), software patch management (16), use of digital signature and encryption systems (17), secure application development (22) and effective incident management and response (10) are essential pre-conditions to acquire capabilities for cyber security.

These achieved capabilities (showed as level II issues in Figure 3) as a result of processes put in place are: adoption of data-driven cyber security investment decisions (7) by demonstrating return on investment, hiring of benchmarked security staff (8), training and security awareness of employees (4) and, finally, ability to defend against malware (3) and analyze security breaches for corrective action (9).

The above indicated capabilities of the organization help in achieving its final goal (showed as level I issues in Figure 3), viz. information theft issues (24), business continuity (6) and disaster preparedness (5).

5. Discussion and managerial insight

The fast emerging breed of new generation malware brings an urgency and helplessness to the security managers and makes cyber security a challenge to the organizations using information and communication technology (ICT) for their core functions. The three pillars of information security, viz. confidentiality, integrity and availability are essential for protecting privileged information and business continuity during manmade or natural disasters. This feature can be achieved by designing survivability and resilience in the organization's critical information infrastructure. Unless top management is convinced of the business value of security investment and perceives this investment as essential to meet legal and regulatory norms, the required funding for the cyber security would not be forthcoming. Any holistic approach to cyber security would have to factor these issues.

We get to see these dependency linkages in the Indian context by critically examining the evolution of e-Governance systems (Figure 1) by Gupta (2010) starting from the decade of 1960 when the inadequacy of the existing telecommunication infrastructure in India during the war with China in 1962 triggered the process of revamping this sector. It was the realization at the Indian government level (top management support at the national level) that resulted in early initiatives. However, no effective regulatory and legal framework was put in place specifically dealing with evolving ICT infrastructure through the decades of 1970 and 1980. Close to 25 crucial years went by before the compulsions of an era of globalization gave birth to "Liberalization Era" in the decade beginning 1990. The software export market and birth of e-Governance highlighted the need for regulatory and legal framework. The IT Act 2000 was born out of these compulsions. The increasingly networked systems and rise in incidents of cyber crime around the world did not leave India unaffected. Again the gaps in the IT Act 2000 to address the emerging cyber crime challenges although understood did not result in

necessary amendments in the Act till 2008. The reasons are not far to seek. The amendments to the IT Act in 2008 essentially made it necessary for the government and the industry to follow cyber security good practices to meet emerging threats. The effort and expenditure to achieve the required security posture was being resisted by the stakeholders because of the urge to maintain the status quo. The passage of this amended IT Act was enabled because of availability of international cyber security standards like ISO/IEC 27002 and cyber security governance models in developed countries. These countries outsourcing their IT-related work to Indian industry were insisting on these best practices being followed by their Indian partners. The economic incentive and availability of cyber security standards and governance models provided the thrust for the revision of the IT Act to align its provisions to real-world challenges.

While evaluating the hierarchical structure of issues evolved through this research, it is helpful in viewing the cyber security in terms of leading, coincident and lagging indicators, similar to economic indicators. While a coincident indicator reflects current security conditions, leading and lagging indicators reflect security conditions that existed before and after a shift in security efforts, respectively. Clarity on the type of an indicator is important. A lagging security indicator with a short lag time is preferred, as one can relate it readily with the corresponding leading indicator that is causing it. The hierarchical structure (Figure 3) created using ISM brings distinction between leading and lagging indicators. The level V variables are leading indicators compared with levels I and II variables. It implies that presence of lagging variable depends on leading variable, and even if, for example, top management support (1) is withdrawn, the levels I and II variables may continue to be manifested for sometime as they are lagging variables. Stoppage of watering the roots would show an effect on the condition of branches after some elapsed time. Cyber security governance at national level, international cyber security treaties, regulatory and legal frameworks, risk management in conformity with international standards and top management support are examples of leading indicators. There can be no sustainable cyber security at national level without these leading indicators.

India, as a developing country, appears to be at levels V and IV, where national strategy of cyber security and legal framework is articulated. ISO/IEC 27002 has been adopted as the security standard[1], and alignment of the IT Act 2000 to the emerging cyber security challenges has been attempted by amendments in February 2009 and formulation of rules under the Act (DSCI, 2010). Creation of processes has stabilized in some premier IT companies and financial sector to ensure mandatory compliance with relevant cyber security standards (DSCI, 2010). With the declaration of National Cyber Security Policy[2], proactive regulatory framework and matching capability in law enforcement agencies would provide the nurturing environment to mitigate cyber threat.

5.1 International value of the findings

Effective information security initiatives have to view both technical and social aspects. While technical solutions keep evolving to counter the emerging threats, the social aspects are anchored in the social dynamics and present bigger challenges. The governments and organizations tend to emphasize technical solutions because they can be implemented with ease if adequate funding is provided. Social aspects need change in mindset and restructuring of the regulatory framework. We cannot achieve sustainable

cyber security without a balance of the two. The challenge of social aspect is common to both developed and developing countries. This explains the fact that despite adequate funding, the cyber security continues to be a challenge for developed countries also. New issues of policy and law appear continuously as technological innovations shape the way society communicates, leaving policymakers and concerned legislators trailing behind. The insights generated by this paper may benefit cyber security initiatives of other nations, and the Indian context is only serving as an illustration. It is true that the degree of ICT penetration or Internet usage would vary from country to country, and even if cyber security problems are similar, the way to deal with those problems will depend on local culture, contexts and national legal frameworks. Even with these differences, some countries at a regional level might have the same level of Internet penetration and similar cyber security needs. Any global strategy to develop a cyber security culture has to be adapted to local needs. When developing cyber security culture, one of the main challenges is to segregate the global and international issues from the local issues. International standards can only contribute to identifying the global and generic main issues related to a cyber security culture. The concept of "cyber security maturity continuum" acknowledges this reality while implementing the cyber security programs at organizational or national level (NIST, 2008). The journey to cyber security and resilient information infrastructure has to be traversed through the maturity continuum starting at levels V and IV (Figure 3) where national and organizational strategies of cyber security and legal frameworks are articulated, and this corresponds with the starting maturity level of goals and objective setting. The creation of processes and ensuring compliance at level III corresponds to the maturity level of implementation. The availability of cyber security capabilities at level II leads to next stage of maturity where one can measure efficiency and effectiveness of the processes put in place in the previous stage. The fruits of cyber secure and resilient information infrastructure can be ours only by following these stages in the correct order. We need to resist the tendency to use technology-driven solutions only. Technology is important but impotent without supporting processes and nurturing regulatory and legal framework.

This research using Delphi and ISM methodologies has illustrated an option to segregate the information security issues in distinct five levels of national, organizational, processes, capabilities and final objective of a cyber secure nation. It seems possible to reach useful country-specific insights by identification and prioritization of the information security issues by impaneling cyber security experts from various sectors, viz. government, private, academic and legal, of the country of research. The common factors emerging from this approach across illustrative nations may help in guiding international efforts by United Nations and other regional alliances.

5.2 Implications for research

Highlight of this research is ingenious deployment of two idea engineering methods in developing interpretable structural model of 25 information security issues. This model provides valuable insights and can guide the policy formulation. This is the key contribution of this paper. It hardly needs any emphasis on the need for continuous search of all technical and social issues and formulating policies and programs using experts' judgment in a rigorous manner. Subsequent research may scale up to the global level for extension and validation by impaneling Delphi experts from nations belonging

to different regions. Time-variant analysis can be attempted with the help of System Dynamics modeling using causal loop diagrams (CLDs) to account for the supportive and inhibiting influence of various issues. This approach has the potential to generate more realistic insights that can inform policy formulation.

The structuring of the 25 security issues in five distinct levels, viz. strategic, tactical, process, capability and end objectives, while viewing their relationship using the metaphor of a tree, viz. root, trunk, branches, leaves and fruits, is helpful to appreciate their symbiotic relationship. Similarly viewing the cyber security in terms of leading, coincident and lagging indicators is an interesting concept. The level V variables are leading indicators compared with levels I and II variables. All levels are equally important and one cannot be ignored at the cost of other.

The current research trends emphasizing equal importance of the social and management dimension besides technical processes and technology artifacts. This seems to validate the insights generated by our research.

5.3 Implications for practice

It brings about key information security issues connected with its various facets, viz. national-/organizational-level initiatives, supportive processes, capabilities and objectives. These issues, identified by Indian experts in the Indian context offer a method that one could apply in other national contexts and see whether substantial differences occur, and how other experts prioritize these issues. The analysis of social issues along with technical issues using the ISM tool provides us insights that are considered applicable to a larger context than India. The policy and program formulations in other nations can benefit from the insights generated by this research. The fast-paced proliferation of technology and its resultant vulnerabilities have given birth to an underground economy of malware trading by criminals, terrorists and hostile nation states. Secure cyber space for legitimate use by the globalized world can only be achieved by international cooperation. We cannot afford "digital divide" in cyber defense. As explained earlier, cyber security is a challenge for both developed and developing nations. Prioritization of our resources in a sequence suggested by ISM analysis would help us face the challenge of cyber security better. The methodology suggested in this paper would ensure adequate response to cyber threats and eliminate *ad hoc* reaction.

6. Concluding remarks

The analysis using ISM has provided interesting managerial insights. The model categorizes the variables in five levels. Level V has the highest driving power and least dependence. Variables at this level are national-level policies and strategies which are a precondition for organizational-level policies at level IV. The variables at these levels can be considered to be the foundation of cyber security edifice. It is imperative to build strong fundamentals to build the theory and practice of National Information Security. The cyber security processes at level III cannot sustain without level IV support. The capabilities to secure cyber space at level II come from the underlying processes. The final objective of securing privileged information and creating a resilient organization capable of carrying on its business under all threats (level I) is achieved only after putting in place the underlying edifice. It is not advisable to skip any of the levels to achieve a process-driven national information security. This paper has provided a

perspective on relative importance and priority level of various issues connected with cyber security and provided the basics of a process-driven measurement of achieved national information security. Future work toward identification of variables indicative of these issues would help us in applying suitable weight while designing an index of information security in the Indian context. The insight generated by the hierarchical relationship of the cyber security issues can guide India's effort to create cost-effective cyber security infrastructure. Foundation has been laid by amendment to the IT Act 2000 in February 2009, adoption of ISO/IEC 27002 as the basic framework to guide nation's cyber security effort and declaration of national cyber security policy in 2013. While the paper has used the Indian context as illustrative to analyze the issues identified by Indian security experts, the applicability of its findings is global. It is akin to laws of physics which are independent of geographical location while trying to reach escape velocity. The challenge, while attempting to reach escape velocity in cyber security, is to be sensitive to stages that necessarily need to be traversed and in the correct order to reach the final objective of secure cyber world. The paper has used ISM methodology to structure the policy-making framework for cyber domain. In future research, use of CLD approach and extending it to an international context may provide more realistic insights for policy formulation.

Notes

1. Ministry of Information and Communication Technology, http://mit.gov.in/default.aspx (accessed June 2011).
2. Department of Electronics and Information Technology, http://deity.gov.in/content/national-cyber-security-policy-2013-1 (accessed December 2013).

References

Anderson, E.E. and Choobineh, J. (2008), "Enterprise information security strategies", *Computers & Security*, Vol. 27 Nos 1/2, pp. 22-29.

Attri, R., Dev, N. and Sharma, V. (2013), "Interpretive structural modelling (ISM) approach: an overview", *Research Journal of Management Sciences*, Vol. 2 No. 2, pp. 3-8.

Bajaj, K. (2010), *The Cybersecurity Agenda – Mobilizing for International Action*, The EastWest Institute, New York, NY, available at: www.ewi.info (accessed June 2013).

BIC (2013), "D2.5 - final report of the working groups activities", Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services, available at: www.bic-trust.eu

Bolaños, R., Fontela, R.E. and Pastor, P. (2005), "Using interpretive structural modeling in strategic decision-making groups", *Management Decision*, Vol. 43 Nos 5/6, pp. 877-895.

Brand, D.H. Jr, Irwin, D.M. and Kawamura, K. (1976), "Implementation of interpretive structural modeling in a state-level planning context", in *Seventh Annual Pittsburgh Conference on Modeling and Simulation, Pittsburgh, PA*.

Catrantzos, N. (2010), "No dark corners: a different answer to insider threats", *Homeland Security Affairs*, Vol. VI No. 2, available at: www.hsaj.org

Chang, K.C. and Wang, C.P. (2011), "Information systems resources and information security", *Information System Frontiers*, Vol. 13 No. 4, pp. 579-593.

Choo, K.K.R. (2011), "The cyber threat landscape: challenges and future research directions", *Computers & Security*, Vol. 30 No. 8, pp. 719-731.

CISCO (2011), "Next-generation networks: security for today and tomorrow", available at: www.cisco.com/en/US/solutions/collateral/ns1168/IDG_CSO.pdf (accessed 17 December 2011).

Colwill, C. (2009), "Human factors in information security: the insider threat – who can you trust these days?", *Information Security Technical Report*, Vol. 14 No. 4, pp. 186-196.

Cyberspace Policy Review (2009), "Assuring a trusted and resilient information and communications infrastructure", available at: www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed November 2010).

Dalkey, N. and Helmer, O. (1963), "An experimental application of the Delphi Method to the use of experts", *Management Science*, Vol. 9 No. 3, pp. 458-467.

DHS (2009), "A roadmap for cybersecurity research", Department of Homeland Security, available at: www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf (accessed May 2010).

Dogrul, M., Aslan, A. and Celik, E. (2011), "Developing an international cooperation on cyber defense and deterrence against cyber terrorism", in Czosseck, C., Tyugu, E. and Wingfield, T. (Eds), *3rd International Conference on Cyber Conflict*, CCD COE Publications, Tallinn.

DSCI (2010), "Data security council of India", available at: www.dsci.com.in (accessed February 2010).

Forsyth, J.M. (2013), "What great powers make it: international order and the logic of cooperation in cyberspace", *Strategic Studies Quarterly*, Vol. 7 No. 1, p. 93.

Geers, K. (2010a), "The challenge of cyber attack deterrence", *Computer Law & Security Review*, Vol. 26 No. 3, pp. 298-303.

Gerber, M. and von Solms, R. (2008), "Information security requirements – interpreting the legal aspects", *Computers & Security*, Vol. 27 Nos 5/6, pp. 124-135.

Goel, S. and ChengalurSmith, I.N. (2010), "Metrics for characterizing the form of security policies", *Journal of Strategic Information Systems*, Vol. 19 No. 4, pp. 281-295.

Gordon, T.J. and Helmer, O. (1964), *Report on a Long-range Forecasting Study*, The Rand Corporation P-2982, Santa Monica, CA.

Gupta, M.P. (2010), "Tracking the evolution of E-Governance in India", *International Journal of Electronic Governance Research*, Vol. 6 No. 1, pp. 46-58.

Gupta, M.P., Kumar, P. and Bhattacharya, J. (2004), *Government Online: Opportunities and Challenges*, TMH, New Delhi, pp. 366-421.

Hart, W.L. and Malone, D.W. (1974), "Goal setting for a state environmental agency", in *IEEE Conference on Decision and Control*, *Phoenix, AZ*.

Hawthorne, R.W. and Sage, A.P. (1975), "On applications of interpretive structural modelling to higher education program planning", *Socio-Economic Planning Sciences*, Vol. 9 No. 1, pp. 31-43.

IWM-SF (Information Warfare Monitor & Shadowserver Foundation) (2010), "Shadows in the cloud: investigating cyber espionage 2.0", available at: www.nartv.org/mirror/shadows-in-the-cloud.pdf (accessed June 2013).

Jharkharia, S. and Shankar, R. (2004), "IT enablement of supply chains: modeling the enablers", *International Journal of Productivity and Performance Management*, Vol. 53 No. 8, pp. 700-712.

Jung, O., Berger, A., Hirschbichler, M., Gojmerac, I., Lippitsch, H., Tscherwenka, M. and Umschaden, K. (2010), "IMS security and what we should learn from the internet", *Elektrotechnik & Informationstechnik*, Vol. 127 No. 5, pp. 116-120.

Kannan, G. and Haq, N.A. (2007), "Analysis of interactions of criteria and sub-criteria for the selection of supplier in the built-in-order supply chain environment", *International Journal of Production Research*, Vol. 45 No. 17, pp. 1-22.

Kawamura, K. and Christakis, A.N. (1976), "The role of structural modeling in technology assessment", in *Second International Congress on Technology Assessment was held at The University of Michigan, Ann Arbor (USA) in October, 1976*.

Keeney, S., Hasson, F. and McKenna, H.P. (2001), "A critical review of the Delphi technique as a research methodology for nursing", *International Journal of Nursing Studies*, Vol. 38 No. 2, pp. 195-200.

Knapp, K.J., Morris, R.F., Marshall, T.E. and Byrd, T.A. (2009), "Information security policy: an organizational-level process model", *computers & security*, Vol. 28 No. 2009, pp. 493-508.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: a threat avoidance perspective", *Journal of Association for Information Systems*, Vol. 11 No. 7, pp. 394-413.

Linstone, H.A. and Turoff, M. (Eds) (1975), *The Delphi Method, Techniques and Applications*, Addison–Wesley, Reading, MA.

McCrohan, K.F., Engel, K. and Harvey, J.W. (2010), "Influence of awareness and training on cyber security", *Journal of Internet Commerce*, Vol. 9 No. 1, pp. 23-41.

Mandal, A. and Deshmukh, S.G. (1993), "Vendor selection using interpretative structural modeling", *International Journal of Operations & Productions Management*, Vol. 14 No. 6, pp. 52-59.

Martin, N. and Rice, J. (2011), "Cybercrime: understanding and addressing the concerns of stakeholders", *Computers & Security*, Vol. 30 No. 8, pp. 803-814.

National Cyber Security Policy (2011), "India's national cyber security policy draft v1.0", 26 March, available at: www.mit.gov.in (accessed August 2011).

National Security Threats in Cyberspace (2009), "American bar association standing committee on law and national security workshop report", September 2009, available at: www.thehalocorp.com (accessed May 2013).

Navare, J. and Gemikonakli, O. (2010), "Governance and risk management of network and information security: the role of public private partnerships in managing the existing and emerging risks", in Tenreiro de Magalhães, S., Jahankhani, H. and Hessami, A.G. (Eds), *Global, Security, Safety, and Sustainability: ICGS3 2010, CCIS 92*, Springer-Verlag, Berlin, Heidelberg, pp. 170-177.

Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012), "SCADA security in the light of Cyber-Warfare", *Computers & Security*, Vol. 31 No. 4, pp. 418-436.

NIST (2008), "Performance measurement guide for information security", NIST Special Publication 800-55 Revision 1, July 2008, available at: www.csrc.nist.gov/publications/nistpubs/800-55rev1/sp800-55.pdf (accessed May 2010).

Oliver, W.M. (2009), "Policing for homeland security: policy and research", *Criminal Justice Policy Review*, Vol. 20 No. 3, pp. 253-260.

ORF (2013), "ORF cyber monitor", August 2013, available at: http://orfonline.org/cms/sites/orfonline/html/cyber/cybsec1.html

Parente, F.J., Anderson, J.K., Myers, P. and O'Brien, T. (1984), "An examination of the factors contributing to Delphi accuracy", *Journal of Forecasting*, Vol. 3 No. 2, pp. 173-182.

Polónia, F. and de Sá-Soares, F. (2013), "Key issues in information systems security management, ICIS 2013", available at: http://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/3/

Ravi, V. and Shankar, R. (2005), "Analysis of interactions among the barriers of reverse logistics", *Technological Forecasting and Social Change*, Vol. 72 No. 8, pp. 1011-1029.

Rowe, G. and Wright, G. (1999), "The Delphi technique as a forecasting tool: issues and analysis", *International Journal of Forecasting*, Vol. 15 No. 4, pp. 353-375.

Sharkey, S. (2001), "An approach to consensus building the Delphi technique: developing a learning resource in mental health", *Nurse Education Today*, Vol. 21 No. 5, pp. 398-408.

Shin, D. (2010), "A socio-technical framework for cyber-infrastructure design implication for Korean cyber-infrastructure vision", *Technological Forecasting & Social Change*, Vol. 77 No. 5, pp. 783-795.

Sushil (2005), "Interpretive matrix: a tool to aid interpretation of management and social research", *Global Journal of Flexible Systems Management*, Vol. 6 No. 2, pp. 27-30.

The Guardian (2013), "NSA spied on Indian embassy and UN mission, Edward Snowden files reveal", article by Jason Burke, South Asia correspondent of *The Guardian*, 25 September, available at: www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission

The Hindu (2013), "NSA puts cyber security initiative on fast track", *The Hindu*, 20 July, available at: www.thehindu.com/news/national/nsa-puts-cyber-security-initiative-on-fast-track/article4933077.ece

Torres, J.M., Sarriegi, J.M., Hernantes, J. and Lauge, A. (2009), "Steering security through measurement", in Fischer-Hübner, S., Lambrinoudakis, C. and Pernul, G. (Eds), *Trust, Privacy and Security in Digital Business: TrustBus 2009, LNCS 5695*, Springer-Verlag, Berlin, Heidelberg, pp. 95-104.

Turoff, M. (1970), "The design of a policy Delphi", *Technological Forecasting and Social Change*, Vol. 2 No. 2, pp. 149-171.

Warfield, J.W. (1974), "Developing interconnected matrices in structural modeling", *IEEE Transactions on Systems Men and Cybernatics*, Vol. 4 No. 2, pp. 51-81.

Westby, J.R. (2010), "Governance of enterprise security: CyLab 2010 report", Carnegie Mellon CyLab, Carnegie Mellon University, available at: www.federalnewsradio.com/docs/070810_cmu_rept.pdf (accessed May 2011).

Williams, P.L. and Webb, C. (1994), "The Delphi technique: a methodological discussion", *Journal of Advanced Nursing*, Vol. 19 No. 1, pp. 180-186.

You, N., Kato, Y. and Kitaoka, M. (1994), "Numerous date in hierarchy for knowledge concentrated in decision tree", *Computers & Industrial Engineering*, Vol. 27 Nos 1/4, pp. 535-538.

Further reading

ENISA Threat Landscape (2012), "ENISA threat landscape, responding to the evolving threat environment", available at: www.enisa.europa.eu (accessed June 2013).

Furnell, S.M. and Clarke, N.L. (2005), "Organisational security culture: embedding security awareness, education and training", *Proceedings of the 4th World Conference on Information Security Education (WISE 2005)*, *Moscow*, *18-20 May*.

Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002), "A prototype tool for informationsecurity awareness and training", *Logistics Information Management*, Vol. 15 Nos 5/6, pp. 352-357.

Geers, K. (2010b), "Cyber weapons convention", *Computer Law & Security Review*, Vol. 26 No. 5, pp. 547-551.

Hawkins, S., Yen, D.C. and Chou, D.C. (2000), "Awareness and challenges of internet security", *Information Management & Computer Security*, Vol. 8 No. 3, pp. 131-143.

Ku, C.Y., Chang, Y.W. and Yen, D.C. (2009), "National information security policy and its implementation: a case study in Taiwan", *Telecommunications Policy*, Vol. 33 No. 7, pp. 371-384.

Spurling, P. (1995), "Promoting security awareness and commitment", *Information Management & Computer Security*, Vol. 3 No. 2, pp. 20-26.

Appendix

Steps involved in ISM methodology

ISM uses systematic application of some elementary notions of graph theory and Boolean algebra in such a way that when implemented in a man–machine interactive mode, theoretical, conceptual and computational leverage is exploited to construct a directed graph (a representation of the hierarchical structure of the system) (Attri *et al.*, 2013). The various steps involved in ISM modeling as described in Figure A1 are given below:

- Identify the elements which are relevant to the problem. This could be done by a survey or group problem-solving technique (we have used Delphi methodology).
- Establish a contextual relationship between elements with respect to which pairs of elements would be examined.
- Develop a structural self-interaction matrix (SSIM) of elements. This matrix indicates the pairwise relationship among elements of the system. This matrix is checked for transitivity. For this purpose, experts from the industry and academia should be consulted in identifying the nature of contextual relationship among the factors. These experts from the industry and academia should be well conversant with the problem under consideration. For analyzing the factors, a contextual relationship of "leads to" or "influences" type must be chosen. This means that one factor influences another factor. On the basis of this, contextual relationship between the identified factors is developed. The following four symbols are used to denote the direction of relationship between two factors (i and j): V for the relation from factor i to factor j (i.e. factor i will influence factor j); for the relation from factor j to factor i (i.e. factor i will be influenced by factor j); X for both direction relations (i.e. factors i and j will influence each other); and O for no relation between the factors (i.e. barriers i and j are unrelated).
- Develop a reachability matrix from the SSIM. For this, SSIM is converted into the initial reachability matrix by substituting the four symbols (i.e. V, A, X or O) of SSIM by 1 s or 0 s in the initial reachability matrix. The rules for this substitution are as follows: If the (i, j) entry in the SSIM is V, then the (i, j) entry in the reachability matrix becomes 1 and the (j, i) entry becomes 0; if the (i, j) entry in the SSIM is A, then the (i, j) entry in the matrix becomes 0 and the (j, i) entry becomes 1; if the (i, j) entry in the SSIM is X, then the (i, j) entry in the matrix becomes 1 and the (j, i) entry also becomes 1; if the (i, j) entry in the SSIM is O, then the (i, j) entry in the matrix becomes 0 and the (j, i) entry also becomes 0.
- Partition the reachability matrix into different levels. From the final reachability matrix, for each factor, reachability set and antecedent sets are derived. The reachability set consists of the factor itself and the other factor that it may impact, whereas the antecedent set consists of the factor itself and the other factor that may impact it. Thereafter, the intersection of these sets is derived for all the factors, and levels of different factor are determined. The factors for which the reachability and the intersection sets are the same occupy the top level in the ISM hierarchy. The top-level factors are those factors that will not lead the other factors above their own level in the hierarchy. Once the top-level factor is identified, it is removed from consideration. Then, the same process is repeated to find out the factors in the next level. This process is continued until the level of each factor is found. These levels help in building the diagraph and the ISM model.

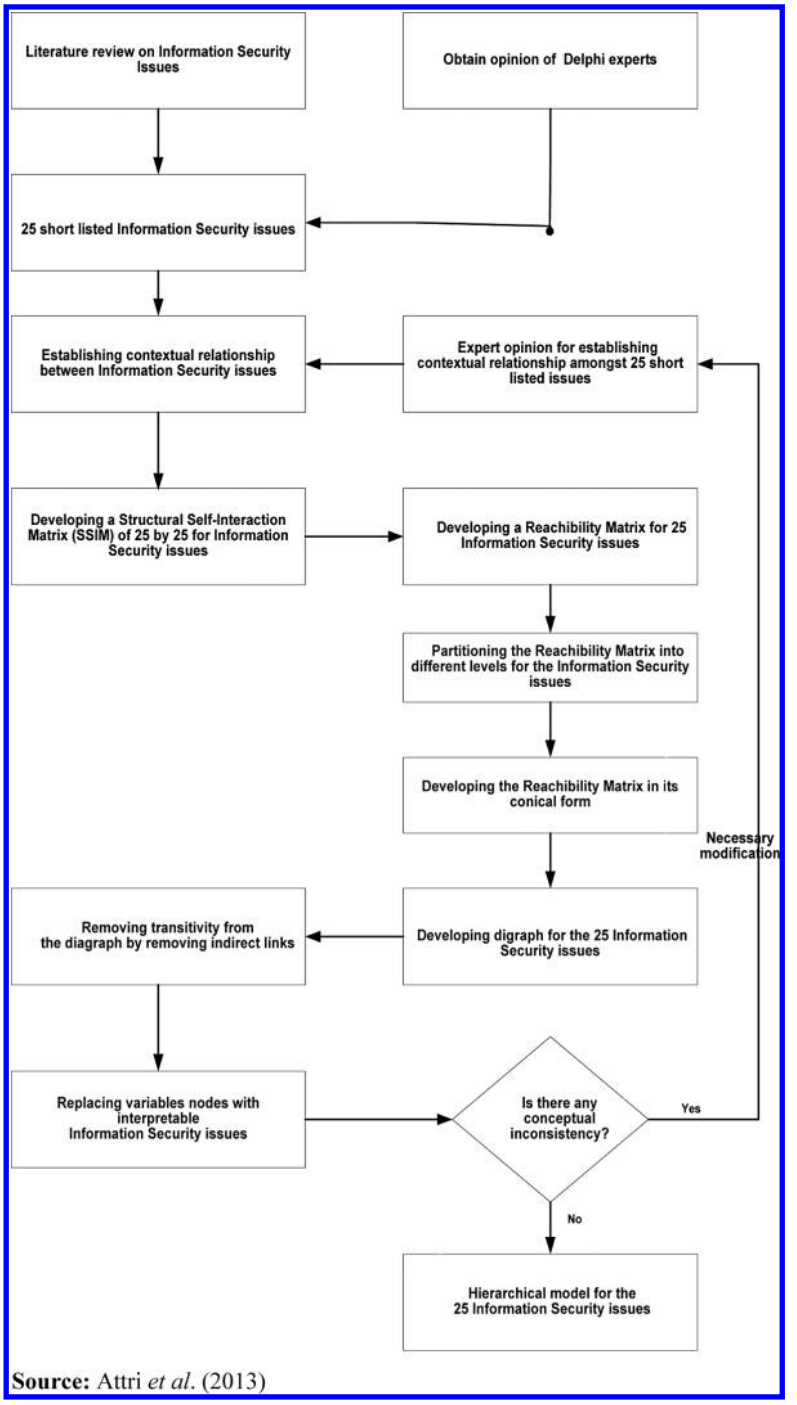


Figure A1.
Flow diagram for preparing the ISM model

- Convert the reachability matrix into a conical form. The Conical matrix is developed by clustering factors in the same level across the rows and columns of the final reachability matrix. The drive power of a factor is derived by summing up the number of ones in the rows and its dependence power by summing up the number of ones in the columns14, 15 and 16. Next, drive power and dependence power ranks are calculated by giving highest ranks to the factors that have the maximum number of ones in the rows and columns.
- Draw a digraph based on the relationship given in the reachability matrix and remove transitive links. In this development, the top-level factor is positioned at the top of the digraph and the second-level factor is placed at the second position and so on, until the bottom level is placed at the lowest position in the digraph.
- Convert the resultant digraph into an ISM-based model by replacing element nodes with the statements.
- Review the model to check for conceptual inconsistency and make the necessary modifications.

About the authors

Manmohan Chaturvedi is a Professor at Ansal University, Gurgaon, and a retired Indian Air Force (IAF) officer with PhD in Information Security from IIT Delhi. He has about 35 years of experience in managing technology for the IAF. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with telecommunication policy issues. He graduated from Delhi College of Engineering and completed postgraduation from IIT Delhi. Current interests include vulnerability analysis of evolving ICT infrastructure. Manmohan Chaturvedi is the corresponding author and can be contacted at: mmchat7@gmail.com

Abhishek Narain Singh is a PhD scholar in the Department of Management Studies, Indian Institute of Technology, Delhi, India. Mr Singh holds Masters and Bachelor Degrees in Computer Science and Engineering. His current research interests include information security management and e-Governance. He has presented his research work at national and international forums. He was a visiting scholar to Ludwig-Maximilians-University at Munich in Germany on "Doctoral Student Exchange Program" as a fellow of Deutscher Akademischer Austausch Dienst.

Manmohan Prasad Gupta is Chair-Information Systems Group and Coordinator-Center for Excellence in e-Governance at the Department of Management Studies, Indian Institute of Technology, Delhi. With research interests in the areas of IS/IT planning and e-Government, Prof Gupta has authored the acclaimed book "Government Online" and edited two others entitled "Towards E-Government" and "Promise of E-Government", published by McGraw Hill, 2005. He was the recipient of the prestigious Humanities and Social Sciences (HSS) fellowship of Shastri Indo-Canadian Institute, Calgary (Canada), and a Visiting Fellow at the University of Manitoba.

Jaijit Bhattacharya is an e-Governance expert and is Adjunct Professor at IIT Delhi and President of Centre for Digital Economy Policy Research (C-DEP). He is also Director, Government Affairs, Hewlett Packard. Dr Bhattacharya did his PhD from Department of Computer Science, IIT Delhi, MBA from IIM Calcutta and BTech in Electrical Engineering from IIT Kanpur.