The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1741-0398.htm

Received 20 July 2013
Revised 27 August 2013
11 September 2013
Accepted 11 September 2013

Identifying factors of "organizational information security management"

Abhishek Narain Singh and M.P. Gupta
Department of Management Studies, Indian Institute of Technology Delhi, New Delhi, India, and
Amitabh Ojha
Research Design and Standards Organization, Ministry of Railway, Government of India, Lucknow, India

Abstract

Purpose – Despite many technically sophisticated solutions, managing information security has remained a persistent challenge for organizations. Emerging IT/ICT media have posed new security challenges to business information and information assets. It is felt that technical solutions alone are not sufficient to address the information security challenge. It has been argued that organizations also need to consider the management aspects of information security. Consequently, literature, especially in the last decade, has witnessed various scholarly works in this direction. Therefore, a synthesis exercise is required to bring clarity on categorizing the issues of organizational information security management (ISM) to take the research forward. The purpose of this paper is to identify management factors that address organizational information security challenges.

Design/methodology/approach – Using a mix method approach, the paper adopts the qualitative (keyword analysis and experts' opinion) and quantitative (questionnaire survey) research routes. Exploratory factor analysis is conducted to find out the key factors of organizational ISM.

Findings – The paper categorizes various organizational ISM functions into ten factors. Spanning across three levels (strategic, tactical and operational), these factors cover various management issues of organizational ISM.

Originality/value – The paper takes the ISM literature forward by statistically validating the key management factors of organizational ISM. The study outcome should help to draw the attention of organizations toward the managerial challenges of organizational ISM.

Keywords Organizations, Information security, Information security management, Information security management system, Management factors

Paper type Research paper

1. Introduction

Increasing dependence of businesses on information and organizational information assets has created a burning need for information security. The current era of rapid technological advancements has posed new threats to business information and information assets at every stage of information life cycle (i.e. information generation, processing, storage and distribution) for organizations. Many high-end technological solutions have been proposed and implemented to deal with this situation. However, information security still remains a serious challenge. A permanent lag in addressing this issue at strategic and tactical levels within organizations is the primary reason for such a state of affairs (von Solms and von Solms, 2004; Ma *et al.*, 2009). Therefore, it can be argued that addressing information security challenges is not merely a technical issue, the management and behavioral aspects are also of pivotal importance but are often overlooked by organizations.

Journal of Enterprise Information Management
Vol. 27 No. 5, 2014
pp. 644-667

1741-0398
DOI 10.1108/JEIM-07-2013-0052

Information security discipline has matured over a period of time with the changing nature of information usage for business purposes, dependence of businesses on information systems and accordingly varying risk/threat scenarios. As described by von Solms (2000, 2006), the information security management (ISM) literature has transited through four waves: technical wave, management wave, institutional wave and governance wave. This study is an attempt to fill the literature gap by focussing on management wave and the way it further encompasses institutional and governance perspectives of organizational ISM.

The next section of the paper discusses existing literature in the area, broadly under key frameworks and factors of organizational ISM. Further, the paper describes the methodology adopted. A mix of qualitative (keyword analysis and experts' opinion) and quantitative (questionnaire based survey) research methods were used to provide rigor. The subsequent section presents results and discusses the identified factors of organizational ISM. Finally, the paper presents the implications of research findings, limitations of the study and the avenues for future research.

2. Literature review

Information security has been defined from multiple perspectives. For example, one of the definitions is: "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide *confidentiality*, *integrity*, and *availability*" (NIST, 2004). Hong *et al.* (2006) described information security as the application of technical methods and managerial processes on the information resources (hardware, software and data) in order to keep organizational assets and personal privacy protected. Therefore, information security is a multidimensional discipline that helps to mitigate the risk to information through the application of an appropriate mix (physical, technical or operational) of security controls (Posthumus and von Solms, 2004). The scope of the present literature review covers ISM and the various factors related to organizational ISM.

2.1 ISM

ISM comprises the set of activities involved in configuring resources in order to meet the information security needs of an organization. The core objective of ISM is to align security objectives to business needs of the organization. The ISO/IEC 27001:2005 (2005) standard defines ISM as that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (ISO/IEC 27001:2005, 2005). This includes the overall concept of organizational policies, planning activities, practices, procedures, processes, etc. Information security is managed at three levels in organizations: strategic (policy driven), tactical (guideline driven) and operational (measures driven) (Eloff and Eloff, 2005). Therefore, an information security management system (ISMS) consists of policies, procedures, guidelines, activities and associated resources, collectively managed by an organization to protect its information assets. It is based upon organization's risk assessment and acceptance levels designed to manage risks effectively. Successful implementation of ISMS is governed by analyzing requirements to protect organizational information assets and apply appropriate security controls to ensure their protection (ISO/IEC 27000:2012, 2012). Scholars (Hong *et al.*, 2003; Posthumus and von Solms, 2004; Eloff and Eloff, 2005; Ma *et al.*, 2009) have suggested different ISM frameworks addressing one or the other aforementioned issues (Table I). For instance, while Posthumus and von Solms (2004) highlight external and

Table I.
ISM frameworks – key factors and research highlights

Reference	Focus	Key factors	Research highlights
Hong *et al.* (2003)	Integrated system theory	Contingency management Security policy Risk management Internal control Information auditing Organizational objectives	*Five-design theories* Security policy theory Risk management theory Control and auditing theory Management system theory, and Contingency theory
Perks and Beveridge (2003)	Information security planning model	*External forces* Current IT environment and opportunities Flexible market situations Changing security threats/vulnerabilities Varying legislative and regulatory environment	*Five steps* Determine current security strategy Evaluate current security strategy against business strategy Desired information security strategy Implement desired information security strategy measure feedback
Posthumus and von Solms (2004)	Information security governance framework	*Internal factors* Business issues and IT infrastructure *External factors* Legal/regulatory issues and standards/best practices	Information security is a corporate governance responsibility
Eloff and Eloff (2005)	Information security architecture	Security policies, standards and procedures Security culture-security awareness and training Monitoring compliance Current security program-risk management Security organization and infrastructure	*Five requirements* Be holistic and encompassing Synchronize different controls to achieve maximum effect A comprehensive approach to information security Risk management Predetermined life cycle Be measurable

(*continued*)

Reference	Focus	Key factors	Research highlights
ISO/IEC 27002:2005 (2005)	Information technology – security techniques – code of practice for information security management	Risk assessment; security policy; information security governance; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; compliance to security policies, standards, laws and regulations	Information security controls and objectives are defined for different aspects of organizational information security management
von Solms and von Solms (2006)	Information security governance model	*Strategic factors* External (legal and regulatory issues, and external risks) Internal (strategic vision, role of IT, alignment of IT with company's strategy, competitiveness, etc.) *Tactical factors* Security policies, standards and procedures *Operational factors* Administrative guidelines and procedures	*Core principle 1* Information security governance happens at three levels, i.e. strategic, tactical and operational *Core principle 2* Three distinct actions, i.e. direct, execute and control at all the three levels
Ma *et al.* (2009)	Integrated framework for ISM	*Five steps* Assess the organizational environment Establish information security objectives Analyze information security requirements Develop information security controls Train/evaluate information security controls	*Four guiding principles* Have goals in mind Align security goals with business strategy ISM is a multivariate system ISM is a dynamic process

(*continued*)

Table I.

Reference	Focus	Key factors	Research highlights
Musa (2010)	Information security governance framework	*External factors* Legal/regulatory Standards/best practices *Internal factors* Business issues IT infrastructure	*Inputs* IT strategy, risk assessment, regulatory requirements and information security baselines *Process* Information security – objectives, policies, standards, guidelines, implementation, mentoring, and performance evaluation *Output* strategic alignment, value delivery, performance measurement, resource management and risk management

Table I.

internal factors such as best practices and regularity compliances for successful implementation of ISM, Musa (2010) describes information security process covering policies, standards, performance evaluation, etc. Therefore, there is a need to organize the multiple and diverse issues of managing information security into logically distinct factors.

2.2 Organizational ISM factors

Scholars have discussed ISM as a multidimensional approach where a range of factors contribute to manage organizational information security needs/requirements. von Solms (2001) identified thirteen such factors. Some of the factors are external in nature, i.e. organizations do not have any control over them, but have to comply or act according to them. Such factors include: current IT environment and opportunities, flexible market situations, changing security threats/risks, legislative and regulatory environment, and industry-wide standards/best practices (Perks and Beveridge, 2003; Musa, 2010). To remain competitive in market and for a smooth business continuity, organizations need to work in accordance with these external forces. In addition, there are also some internal factors that organizations have to control and manage internally, such as: business issues, IT infrastructure, strategic vision and aligning IT with company's strategy, etc. (Posthumus and von Solms, 2004; von Solms and von Solms, 2006). Upfold and Sewry (2005) have identified nine factors that influence ISM practices in small and medium size organizations, namely: security policy, organizational security, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, and business continuity management. In addition to these nine factors, the ISO/IEC 27001:2005 (2005), standard for ISM recommends two more information security controls for organizations, i.e. information security incident management (ISIM) and regulatory compliance (ISO/IEC 27001: 2005, 2005). On similar lines, Chang and Ho (2006) examined various factors (i.e. IT competence, environmental uncertainty, industry type and organization size) that influence the implementation of an ISM standard in organizations. In a survey of 874 Certified Information System Security Professionals (CISSP) across the world, Knapp *et al.* (2006b) reported top 25 technical and non-technical information security challenges faced by organizations globally. Similar human, technical and organizational challenges were also highlighted by Werlinger *et al.* (2009) while conducting 36 semi-structured interviews across seventeen organizations of varying size and nature. As evident from the literature, there are diverse management issues influencing effectiveness of information security in organizations.

3. Research methodology

The objective of this paper is to identify key management factors of organizational ISM and statistically validate them. To achieve this objective, multilevel methodological approach was adopted. First, keyword analysis (Emrouznejad *et al.*, 2008; Kevork and Vrechopoulos, 2009) was conducted to identify the key organizational factors highlighted in the information security literature. Research articles published in the years 2000 onwards in two leading ISM journals *Computers & Security* and *Information Management and Computer Security* were reviewed. In addition, research articles published in the year 2000 onwards in the following outlets were also reviewed: *MIS Quarterly*, *Information & Management*, *Communications of the ACM*, *Computer Fraud & Security*, *Information Security Technical Report*, *Australian Information Security*

Management Conference, and *European Conference on Information Warfare and Security, etc.* Criteria for including a paper in review was that the title of the paper should contain keywords like, "information security," "information risk," "information security management," "data security," "information system security," etc. Using databases such as PROQUEST, SCOPUS and EBSCO, finally 298 research articles were included in the review. In total, 21 most appeared keywords were spotted. At second step, inputs were taken from 24 experts (12 from industry, seven from academia and five from government agencies) to further strengthen and cross-validate the identified key areas of organizational ISM. The practitioners from varied industries with average experience of more than eight years ensured comprehensiveness and reliability of the input. The list of ISM factors as emerging from keyword analysis and experts' opinion is summarized in Table II.

Thus, based on keyword analysis and experts' opinion, ten management factors of organizational ISM are proposed, namely: top management support, information security policy, information security training, information security awareness, information security culture, information security audit, ISM best practices, asset management, information security incident management and information security regulations compliance. Further, micro items for each proposed factor are identified based on existing scales and experts' opinion (Table III). This exercise led to the

Factors	Keyword analysis			
Journal	Computers and security	Information management and computer security	Others	Experts' opinion
Information systems		✓		
Information security	✓		✓	✓
Data security		✓		
Computer security		✓		
Information security management	✓		✓	
Information security management system			✓	✓
Information security policy	✓		✓	✓
Information security education				✓
Security breach/threat/vulnerability	✓	✓		
Information security awareness	✓		✓	✓
Security compliance				✓
Incident management		✓		✓
Information security culture	✓		✓	✓
Asset management		✓		✓
Information security training			✓	✓
Business continuity and disaster management			✓	✓
Information security standards	✓	✓		
ISM best practices			✓	✓
Information security governance	✓			
Certification		✓		
Organizational culture	✓		✓	
Information security audit	✓			✓
Risk assessment/management			✓	✓
Laws/regulations				
Security behavior		✓		✓

Table II.
Exploring ISM factors – keyword analysis and experts' opinion

ISM factors	No. of items	Sources
Top management support	4	Yap *et al.* (1992)
		Yap *et al.* (1992)
		Yap *et al.* (1992)
		Yap *et al.* (1992)
Information security policy	6	Payment Card Industry – Data Security Standards (PCI-DSS) (2010)
		Ma *et al.* (2008)
		PCI-DSS (2010)
		PCI-DSS (2010)
		PCI-DSS (2010)
		PCI-DSS (2010)
Information security training	3	Upfold and Sewry (2005)
		Chang and King (2005)
		Ma *et al.* (2008)
Information security awareness	6	Upfold and Sewry (2005)
		PCI-DSS (2010)
		Musa (2010)
		Upfold and Sewry (2005)
		Upfold and Sewry (2005)
		Upfold and Sewry (2005)
Information security culture	6	Williams *et al.* (2009)
		Williams *et al.* (2009)
		Williams *et al.* (2009)
		Williams *et al.* (2009)
		Williams *et al.* (2009)
		Ma *et al.* (2008)
Information security audit	3	Chang and Lin (2007)
		Developed for the study
		Developed for the study
Information security management best practices	6	Developed for the study
		Upfold and Sewry (2005)
		Ma *et al.* (2008)
		Ma *et al.* (2008)
		Upfold and Sewry (2005)
		Upfold and Sewry (2005)
Asset management	6	Developed for the study
		Developed for the study
		Ma *et al.* (2008)
		Veiga *et al.* (2007)
		Upfold and Sewry (2005)
		Ma *et al.* (2008)
Information security incident management	8	Musa (2010)
		Upfold and Sewry (2005)
		Developed for the study
		Developed for the study
		Ma *et al.* (2008)
		Veiga *et al.* (2007)
		Chang and Lin (2007)
		Upfold and Sewry (2005)
Information security regulations compliance	5	Developed for the study
		Developed for the study
		Developed for the study
		Developed for the study
		Developed for the study

Table III.
Sources of ISM questionnaire items

development of a questionnaire instrument consisting of a total of 53 items. The instrument has two sections. First section comprises questions regarding the ten identified ISM factors. Respondents were asked to reply to questions in this section on a five-point Likert type scale, ranging from "strongly disagree" to "strongly agree." The second section seeks demographic details of respondents. Initial version of the questionnaire was pilot tested with a sample of 55 responses and appropriate revisions were made accordingly. The exploratory factor analysis (EFA) is conducted using principle component analysis and Kaiser's criteria. Factors were rotated by the varimax with Kaiser normalization method.

A total of 936 questionnaires were sent through both, an online link (via e-mail) and offline mode (contacted in-person). Out of 936 sent questionnaires, 165 responses were received. Totally, 13 incomplete responses were discarded and finally, 152 questionnaires were used for final analysis. Organizations from different industries in India such as IT, telecommunication, banking, manufacturing, transportation, etc. were contacted for the questionnaire survey. Target respondents for the survey were employees across the hierarchy and function in organizations. Table IV gives a brief profile of respondents.

4. Results and discussion

The results of EFA exercise show Kaiser-Meyer-Olkin measure of sampling adequacy 0.91. The Bartlett's test of sphericity results was significant at $p = 0.00$. Eigenvalue of each factor were checked and was found exceeding 1. The results show the total accumulated variance of the factors as 68.76 percent. Because of low factor loading values, nine items were dropped. Finally, 44 items were confirmed and categorized into ten factors. Further, to test the reliability of the questionnaire, Cronbach's α value was checked. Internal consistency of the questionnaire was verified using inter-item correlation. Scales in respect of all the ten factors were found reliable, the Cronbach's α values being more than 0.7 (Table V).

Job profile	Frequency	%	Industry type	Frequency	%
Senior executive	9	5.9	IT	75	49.34
System administrator/network manager	9	5.9	Telecommunication	23	15.13
Functional manager	49	32.23	Transport	10	6.58
IT manager	25	16.44	Manufacturing	10	6.58
Information security manager	7	4.60	Consulting	7	4.60
Software engineer/programmer	34	22.36	Banking	6	3.95
Others	19	12.50	Education	4	2.63
Total	152	100	Oil and Gas	4	2.63
			Others	13	8.55
			Total	152	100
Work experience			*Sector*		
<5 years	72	47.36	Public	36	23.68
5-10 years	55	36.18	Private	116	76.31
10-20 years	20	13.15	Total	152	100
>20 years	5	3.29			
Total	152	100			

Table IV.
Profile of the respondents

	FL	EV	PV	CV %	CA
1. Top management support					
Senior executives regard the significance of information security	0.705	5.284	10.361	10.361	0.755
Senior executives attend information security related meetings	0.816				
Senior executives are involved in information security related decisions	0.781				
Senior executives allocate budget and manpower for information security functions	0.561				
2. Information security policy					
My organization has a documented information security policy	0.656	5.217	10.229	20.590	0.862
Information security policy clearly defines information security objectives of the organization	0.715				
Information security policy clearly defines roles and responsibilities of employees	0.739				
Information security policy clearly defines roles and responsibilities of contractors/third party vendors	0.699				
Information security policy is reviewed regularly (or when the environment changes)	0.527				
Procedures for implementing information security policy are clearly defined and documented	0.548				
3. Information security training					
Organization conducts regular information security training for employees	0.601	4.167	8.171	28.761	0.789
Information security training programs offered by the organization are useful	0.611				
There is an information security advisor to coordinate information security functions in the organization	0.683				
4. Information security awareness					
Employees are aware of information security policy and guidelines of the organization	0.730	3.832	7.513	36.274	0.895
Organization conducts programs to make employees aware of the importance of information security	0.504				
Employees' roles and responsibilities for information security are properly communicated	0.592				
Employees are aware that information security incidents must be reported to management immediately (dropped)	–				
Employees are well informed about acceptable and unacceptable usage of information systems and assets	0.696				
Employees are aware of the punishments/disciplinary actions for violating information security guidelines	0.751				
5. Information security culture					
Organization creates an information security focus among all employees	0.604	3.639	7.135	43.409	0.915
Organization makes sure that information security is the first thing on the mind of all employees	0.738				
Organization makes information security the norm for all employees	0.730				
Organization dedicates efforts to create an information security focussed workforce	0.651				
Organization makes sure that all employees are vigilant toward information security	0.664				

(*continued*)

Table V.
Factor and reliability analysis

	FL	EV	PV	CV %	CA
Organization has an information security forum to give management direction and support	0.525				
6. Information security audit					
Organization has a team/committee for conducting information security audits	0.588	3.039	5.960	49.368	0.791
Organization routinely conducts internal information security audits	0.747				
Organization conducts external (third party) information security audits	0.603				
7. Information security management best practices					
Organization has a clean desk policy (dropped)	–	2.653	5.202	54.571	0.740
Anti-virus systems used are up-to-date and are capable to safeguard against viruses	0.608				
Proper authentication is required for external connections	0.555				
Organization follows risk assessment and risk management processes to determine acceptable controls	0.518				
Systems are updated/upgraded according to a structured plan and not in an ad hoc manner (dropped)	–				
Every information security incident is reviewed and report is submitted to the higher management (dropped)	–				
8. Asset management					
Organization makes an inventory record of all the information assets (hardware and software)	0.690	2.638	5.172	59.742	0.789
Different departments/business units of the organization maintain register of critical information assets	0.714				
Information assets are classified on the basis of confidentiality, accountability, usage, etc. (dropped)	–				
The organization protects its information assets adequately (e.g. systems and information) (dropped)	–				
Organization has an access control policy that specifies which users have access to what data	0.600				
Organization has policies requiring compliance with software licenses and prohibiting the use of unauthorized software	0.562				
9. Information security incident management					
Organization has a documented disaster recovery and business continuity plan	0.598	2.483	4.868	64.611	0.885
In the event of a security incident, procedures clearly define what to do and who to call for assistance	0.667				
Organization takes disciplinary action against employees for violating information security rules/norms	0.647				
Disaster recovery and business continuity plan is discussed and communicated to all employees (dropped)	–				
Organization has a backup and recovery process to maintain the integrity and availability of essential information processing and communication services	0.703				
Organization can survive a disaster that may result in the loss of systems, premises, etc.	0.633				
Historical records/data of information misuse/intrusion attempts/data theft are being maintained	0.569				
Information security measures have been reviewed regularly (at least once a year) (dropped)	–				

Table V. (*continued*)

	FL	EV	PV	CV %	CA
10. Information security regulations compliance					
Organization has a data privacy and protection policy (dropped)	–	2.116	4.150	68.761	0.839
Employees have to sign a data privacy and protection agreement	0.579				
Contractors/third party vendors have to sign a data privacy and protection agreement while working with the organization	0.739				
There is a team/committee for monitoring organization's compliance to data protection law/legislation	0.552				
Organization adheres to the industry standards of information security management (e.g. ISO/IEC 27001:2005 (2005), COBIT (2002), etc.)	0.553				

Notes: FL, factor loading; EV, eigenvalue; PV, percentage of variance; CV, cumulative variance (%); CA, Cronbach's α (reliability)

Table V.

The factors identified from the exploratory phase represent organizational ISM activities at all the three levels, i.e. strategic, tactical and operational. Strategic level factors would include top management support (TMS) and information security policy (ISP). These factors are related to policy whereby an organization's information security goals and objectives are defined. At tactical level, the factors are process oriented where various guidelines related to organizational ISM activities are developed. Such factors would include information security training (IST), awareness and culture in the organization. At operational level, factors are measures driven. Consequently, information security audit (ISAudit), asset management and ISM best practices are considered as operational factors. ISIM and information security regulations compliance, however, are regarded as performance factors of organizational ISM which any organization would wish to achieve. Table VI gives the working definition of these factors along with their key issues and select references.

4.1 TMS

A consistent TMS is pivotal for successful implementation of ISM in any organization. ISM is a governance issue and top management must regard its significance (von Solms, 2001; Helle, 2005). Senior executives must participate in ISM related planning and decision-making activities. Involvement of senior management encourages employees to comply with organization's security policies and guidelines (Mouratidis *et al.*, 2008) and helps to create an information security culture (ISC) in the organization (Helle, 2005; Knapp *et al.*, 2006a). Senior management must provide required resources in terms of budget, manpower, technology, etc. to fulfill organizational information security requirements (Williams and Saull, 2001).

4.2 ISP

Having a documented ISP is a first step toward managing information security in any organization. Policy framework should clearly illustrate the information security objectives of the organization and procedures for its implementation (Palmer *et al.*, 2001). The roles and responsibilities for various policy related functions, e.g. policy review, update, monitoring compliance, etc. must be clearly defined (Rees *et al.*, 2003; Knapp *et al.*, 2009). An effective ISP has various elements such as roles/responsibilities

Table VI.
Organizational ISM factors

Factors	Definition	Key issues	References
Top management support	"[…] top management may take the form of guidance during planning, participation during design, involvement during deployment, and encouragement for positive user attitude towards the ISM in organization" (Kankanhalli *et al.*, 2003)	Information security policy compliance Perception of management vs security specialists and employees Security culture and risk management ISM is a corporate government responsibility Information system security effectiveness Provide resources to information security efforts Set up an information security infrastructure	von Solms (2001); Williams and Saull (2001); Dutta and McCrohan (2002); Kankanhalli *et al.* (2003); Helle (2005); Knapp *et al.* (2006a); Mouratidis *et al.* (2008); Hu *et al.* (2012)
Information security policy	"Information security policy provides management direction and support for information security" (ISO/IEC 17799:2000, 2000). "[…] that typically includes general statements of goals, objectives, beliefs ethics and responsibilities; often accompanied by the general means (procedures) for achieving them" (Wood, 1995)	Policy framework Policy elements, characteristics and coverage Formulation, implementation and adoption Information security incident reporting Aligning information security policy with strategic information system plan Employees' behavior toward policy compliance Role of awareness in policy compliance Policy communication Policy effectiveness Policy violations	Palmer *et al.* (2001); Höne and Eloff (2002); Rees *et al.* (2003); Wiant (2005); Doherty and Fulford (2006); Hong *et al.* (2006); Pahnila *et al.* (2007); Bulgurcu *et al.* (2009); Herath and Rao (2009); Bulgurcu *et al.* (2010); Siponen and Vance (2010); Hu *et al.* (2012)
Information security training	"[…] strives to produce relevant and needed information security knowledge and skills, supports competency development, and helps personnel understand and learn how to perform their security roles" (NIST, 2003)	Training needs of personnel Training vs awareness vs education Information security training tool Usefulness of training programs E-learning training module Information security policy compliance	Katsikas (2000); Horrocks (2001); Furnell *et al.* (2002); NIST (2003); Schultz (2004); Eminagaoglu *et al.* (2009); Hagen and Albrechtsen (2009); Puhakainen and Siponen (2010)

(*continued*)

Table VI.

Factors	Definition	Key issues	References
Information security awareness	"[…] is a blended solution of activities that promotes security, establishes accountability, and informs the workforce of information security news" (NIST, 2003)	Requirements, challenges and potential All personnel get the message Dynamic and ongoing process Knowledge and attitude of employees Gap between talk and action Information security behavior Information security policy compliance	Siponen (2001); Furnell *et al.* (2002); Schultz (2004); Peltier (2005); Kruger and Kearney (2006); Emrouznejad *et al.* (2008); Albrechtsen and Hovden (2010); Bulgurcu *et al.* (2009, 2010)
Information security culture	"[…] exists when every participant, appropriately to their role, is aware of the information security risks and preventative measures, assumes responsibility, and takes steps to improve the security of their information systems" (Organisation for Economic Co-operation and Development, 2002)	Employees' information security behavior Attitudes, assumptions, beliefs, values and knowledge of employees and stakeholders Organizational information security culture dimensions Information security policy compliance Organizational culture	Martins and Eloff (2002); Helle (2005); Thomson *et al.* (2006); Knapp *et al.* (2006a); Chang and Lin (2007); Ruighaver *et al.* (2007); Veiga *et al.* (2007); Williams *et al.* (2009); Veiga and Eloff (2010); Hu *et al.* (2012)
Information security audit	"[…] an independent examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures" (NIST, 2011)	Human factor Information systems risk planning Internal audits External (third party) audits Monitor compliance to rules and guidelines	COBIT (2002); Vroom and von Solms (2004); Bedard *et al.* (2005); Humphreys (2008)
Information security management best practices	"[…] the controls specified in various ISM standards applicable to most organizations and readily tailored to accommodate organizations of various sizes and complexities" (ISO/IEC 27000:2012, 2012)	Best practices framework Compliance to ISM standards Competitive advantage Business continuity	Palmer *et al.* (2001); Germain (2005); Ma *et al.* (2008); Tsohou *et al.* (2010)

(*continued*)

Factors	Definition	Key issues	References
Asset management	"[…] identify organizational information assets, associated risks and controls. Asset classification and inventory management is based on ownership and owners should identify acceptable uses" (ISO/IEC 27002:2005, 2005)	Risk assessment Asset classification and control Ownership Threats and protection Physical access control Access control to IT systems/services	BS7799:1999 (1999); Ward and Smith (2002); Veiga *et al.* (2007); Ma *et al.* (2008); Musa (2010)
Information security incident management	"[…] to develop and implement procedures for detecting, reporting, and responding to security incidents; so that, organizations detect incidents quickly, minimize losses, identify weaknesses, and restore operations rapidly" (NIST, 2004)	Risk management Incident management and response Incident information management system Incident response team Business impact Business continuity	Wiant (2005); Upfold and Sewry (2005); Mitropoulos *et al.* (2006); Abimbola (2007); Chang and Lin (2007); Werlinger *et al.* (2009); Herath and Rao (2009); Jarvelainen (2013)
Information security regulations compliance	"[…] to comply with applicable legislation such as copyright, data privacy, protection of financial data and other vital records, rules of evidence, etc. to avoid conflicts and penalties" (ISO/IEC 27002:2005, 2005)	ISM standards Information security laws and regulations Compliance to information security laws/regulations/standards Adherence to organizational information security policies/guidelines	BS 7799:1999 (1999); Höne and Eloff (2002); Posthumus and von Solms (2004); ISO/IEC 27002:2005 (2005); Sundt (2006); Herath and Rao (2009); Bulgurcu *et al.* (2010); Breaux and Baumer (2011)

Table VI.

of employees and contractors/vendors, clause for non-compliance/policy violations, etc. (Höne and Eloff, 2002). Communicating ISP to all the stakeholders is essential for its successful compliance.

4.3 IST

For various emerging professions in the rapidly changing business environment, providing relevant IST to employees is of utmost importance (Horrocks, 2001). Researchers have suggested several approaches such as training, awareness campaigns and educational programs for this (Katsikas, 2000; Horrocks, 2001). A regular IST helps to make employees aware of possible risks/threats to various information assets of the organization and their countermeasures. Thus, such programs help in building an information security informed workforce in the organization. In the literature, there is mention of mismatch between IST programs with the business objectives of organizations such as "fitting a square peg in a round hole" (Schultz, 2004). Therefore, a variety of prototype tools (Furnell *et al.*, 2002) and intervention programs (Hagen and Albrechtsen, 2009; Eminagaoglu *et al.*, 2009) have been suggested to identify and evaluate the usefulness of IST programs offered to employees. Here the role of information security advisor becomes critical in educating/guiding employees for their compliance behavior toward ISPs of the organization (Puhakainen and Siponen, 2010).

4.4 Information security awareness (ISA)

Schultz (2004) highlighted various challenges (e.g. justifying return on investment, direct benefits, usefulness, recognition, etc.) and potentials of ISA programs. It is important to make employees realize the importance and benefits of such programs. To achieve this, Thomson and von Solms (1998) advocated the use of social-psychological principles while designing and implementing ISA programs. For uninterrupted business processes, it is essential to keep employees informed of current security threats, risks and countermeasures. Hence, ISA is an ongoing process that is to be aligned with the changing business requirements and objectives of organization (Kruger and Kearney, 2006). Purpose of such awareness programs is to communicate to employees about organizational ISP, their roles and responsibilities, acceptable usage of organizational information assets/systems and punishments for non-compliance of information security standards of the organization. That ultimately encourages employees' security behavior toward ISP compliance (Albrechtsen and Hovden, 2010; Bulgurcu *et al.*, 2010).

4.5 ISC

The ISC of an organization is about shared beliefs, values and attitudes of employees while interacting with organizational systems and procedures. This helps in creating an information security focussed workforce in the organization so that information security is always at the back of employees' mind and they remain vigilant toward it while performing their day-to-day activities (Williams *et al.*, 2009). The following statement elegantly articulates the point: "An ISC develops due to the information security behavior of employees […]" (Martins and Eloff, 2002). That makes information security a norm for employees. To achieve this, individual-, group- and organizational-level interaction among employees is of pivotal importance (Veiga and Eloff, 2010). This creates a platform to raise concerns and discuss information security issues among employees. It has been argued that ISC is highly associated with the organizational culture (Thomson *et al.*, 2006; Ruighaver *et al.*, 2007).

The way employees perform their daily functions, over a period of time that becomes the culture of the organization; similar is true for ISC.

4.6 ISAudit

ISAudit is considered as an essential dimension of organizational ISM. In the article, "Information security – A multidimensional discipline," von Solms (2001) states: "[…] it is no use having an information security policy, if you cannot determine whether the policy is enforced." Thus, conducting internal as well as external ISAudit is important for an organization to check the compliance of its security policies, guidelines and procedures. There needs to be a clear definition of roles, procedures and timeline for conducting ISAudit in organizations (Humphreys, 2008). Auditing employees' behavior is always a challenge for auditors (Vroom and von Solms, 2004). Periodic external audits by trusted third party are crucial to gain clients' trust that their information is in safe hands.

4.7 ISM best practices

Standards are a mechanism to endorse best practices. Ma *et al.* (2008) have listed a number of ISM best practices provided by different security individuals, standards and organizations. Examples of such best practices are: regular updates of anti-virus software to safeguard systems against virus/malware, proper authentication for external connections, reviewing information security incidents and submitting reports to higher management, etc. Adherence to ISM best practices helps organizations to guard against risks, confirm legal/regulatory compliance, and gain competitive advantage (Germain, 2005). Compliance to ISM best practices gives confidence to employees and increases trust of the partners/clients.

4.8 Asset management

With the increasing dependence of businesses over information systems, information has become one of the most significant business assets for organizations. Thus, protecting such assets against threats is a matter of paramount importance for organizations. Making an inventory record of organizational information assets and classifying assets based on their criticality are the preliminary steps toward asset management. Various key functions of organizational asset management include: asset classification and ownership (BS7799:1999, 1999; Ma *et al.*, 2008), risk assessment (Thomson and von Solms, 1998; Musa, 2010), physical access control (Veiga *et al.*, 2007), and access control to IT systems and services (BS7799:1999, 1999; Ward and Smith, 2002).

4.9 ISIM

In order to respond to information security incidents, organizations need to have a documented ISIM plan (Abimbola, 2007). The plan should clearly specify the roles and responsibilities of employees and the steps to respond to such information security incidents. The document should also contain a disaster recovery and business continuity plan to deal with disaster situations (Werlinger *et al.*, 2009). The incident management and disaster recovery plans should be discussed and proper training should be given to employees. Organizations need to take regular backups of their critical data and processes (Jarvelainen, 2013). Access logs are useful in tracking and post-incident analysis of incidents. Mitropoulos *et al.* (2006) have categorized the information security incidents based on severity and impact, and suggested that post-incident learning is crucial to prevent businesses from such incidents in future.

4.10 Information security regulations compliance

In a fast changing threat scenario and competitive business environment, organizations need to be proactive in protecting their information assets/systems. Thus, adhering to industry standards and complying with information security laws/regulations reflects an organization's commitment in this regard. Examples of it would be a data privacy and protection agreement to be signed by employees, a non-disclosure-agreement for contractors or third party vendors, etc. (Höne and Eloff, 2002). Sundt (2006) discussed various concerns and positive outcomes of compliance to information security laws/regulations. Organizations need to have a standard procedure to confirm their compliance to information security laws/regulations to avoid penalties and legal consequences (Breaux and Baumer, 2011). As per the applicability, multiple ISM industry standards such as ISO/IEC 17799:2000 (2000) (later ISO/IEC 27002:2005, 2005), COBIT (2002), GMITS, etc. are readily available for organizations to adopt.

5. Implications of the research findings

Organizations need to have a balanced mix of technical, management and human aspects of ISM, to effectively address the information security requirements and challenges. Inconsistent support from top management gives a confusing message to employees, thus influences their compliance behavior. Lack of a documented ISP and security culture are common challenges faced by most organizations (Werlinger *et al.*, 2009). Employees are generally unaware of organization's vision/objective of ISM and their roles/responsibilities toward this. Therefore, a documented information security strategy with clearly defined objectives, policies, roles and responsibilities, and employees' acceptable behavior toward organizational information and information assets is a "must" for every organization.

Regular training and awareness programs are helpful in educating employees and thus building a security culture within the organization. Periodic reviews of organizational ISP and guidelines in accordance with changing business environment, current industry standards and legal/regulatory requirements is key to remain competitive in today's business world. Internal ISAudits are useful in this direction as they keep the organization informed of its grey areas. Whereas external audits are useful for verifying the current ISM practices of the organization by a trusted third party, information security certification is helpful for the organization to build a relationship of trust with its clients and partners.

Best practice recommendations work as guiding principles for organizations. Adherence to international ISM best practices gives the organization an assurance that "we are on right track." Organizations need to have a risk management plan to identify and protect their business information assets. In the present complex threat scenario where internal threats are as serious as external, incident management and business continuity planning is crucial. Employees need to be educated on their acceptable behavior and consequences of non-compliance. Sometimes, it is also necessary to take strong action against policy violations to give employees a clear message of the organization's commitment to safeguard its information and related assets.

6. Conclusion, limitations and future work

The present study is motivated by the gaps indicated by previous scholars in the ISM discipline. A key highlighted gap is the practice of treating information security as purely a technical challenge in organizations, giving less attention to the management aspects of it (von Solms and von Solms, 2004; Ruighaver *et al.*, 2007). Despite various

technical solutions, information security incidents still happen and these have led practitioners as well as scholars to realize the relevance of management and behavioral aspects of information security. Thus, a clear transition can be witnessed in the ISM literature in the past decade. ISM is no longer only an IT issue handled by IT department in organizations. Rather, it is now considered as a collective responsibility. In an attempt to synthesize the management aspects of information security, this study identifies the key management factors of organizational ISM.

Though this study makes efforts to adopt multiple research methods to strengthen the validity of the findings, a comparatively larger sample size in questionnaire based survey would have been more useful. Getting information security related data from organizations is a challenge (Musa, 2010). Time and resources are the obvious constraints in getting such data. Furthermore, the responses to identified ISM factors are contextual in nature and therefore, further research effort is required to test the findings in different settings. Second, the present study only aims to identify the management factors of organizational ISM; it does not show how these factors are linked with one another and thereby build a holistic ISM framework for organizations. This opens further avenues for future research.

As an extension of this study, a framework for organizational ISM can be developed based on identified management factors of ISM. Linkages among various factors need to be established to gain insights from the causal relationships among factors. The interplay of various strategic, tactical and operational factors and their effect on performance factors of organizational ISM needs to be investigated. Further, the framework can be validated through empirical studies to verify the conceptual understanding with ground realities. Also, case studies of select organizations from varying industries/sectors can be conducted to explore various organizational ISM practices and to cross examine the identified ISM factors and their linkages among one another.

References

Abimbola, A. (2007), "Information security incident response", *Network Security*, Vol. 2007 No. 12, pp. 10-13.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behavior through dialogue, participation and collective reflection: an intervention study", *Computers & Security*, Vol. 29 No. 8, pp. 432-445.

Bedard, J.C., Graham, L. and Jackson, C. (2005), "Information systems risk and audit planning", *International Journal of Auditing*, Vol. 9 No. 2, pp. 147-163.

Breaux, T.D. and Baumer, D.L. (2011), "Legally 'reasonable' security requirements: a 10-year FTC retrospective", *Computers & Security*, Vol. 30 No. 4, pp. 178-193.

BS7799:1999 (1999), *Information Security Management – Part 1: Code of Practice for Information Security Management*, British Standards Institute, London.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009), "Roles of information security awareness and perceived fairness in information security policy compliance", *Proceedings of the 15th Americas Conference on Information Systems, San Francisco, CA, 6-9 August*.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Chang, E.C. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-361.

Chang, J.C.J. and King, W.R. (2005), "Measuring the performance of information systems: a functional scorecard", *Journal of Management Information Systems*, Vol. 22 No. 1, pp. 85-115.

Chang, S.E. and Lin, C.S. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458.

COBIT (2002), *Control Objectives for Information and Related Technology, by the Information Systems, Audit, and Control Foundation*, Rolling Meadows, ISACA, IL, available at: www.isaca.org/cobit.htm (accessed May 11, 2013).

Doherty, N.F. and Fulford, H. (2006), "Aligning the information security policy with the strategic information systems plan", *Computers & Security*, Vol. 25 No. 1, pp. 55-63.

Dutta, A. and McCrohan, K. (2002), "Management's role in information security in a cyber-economy", *California Management Review*, Vol. 45 No. 1, pp. 67-87.

Eloff, J.H.P. and Eloff, M.M. (2005), "Information security architecture", *Computer Fraud & Security*, Vol. 2005 No. 11, pp. 10-16.

Eminagaoglu, M., Ucar, E. and Eren, S. (2009), "The positive outcomes of information security awareness training in companies – a case study", *Information Security Technical Report*, Vol. 14 No. 4, pp. 223-229.

Emrouznejad, A., Parker, B.R. and Tavares, G. (2008), "Evaluation of research in efficiency and productivity: a survey and analysis of the first 30 years of scholarly literature in DEA", *Socio-Economic Planning Sciences*, Vol. 42 No. 3, pp. 151-157.

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

Germain, R.S. (2005), "Information security management best practice based on ISO/IEC 17799", *The Information Management Journal*, Vol. 39 No. 4, pp. 60-66.

Hagen, J.M. and Albrechtsen, E. (2009), "Effects on employees' information security abilities by e-learning", *Information Management & Computer Security*, Vol. 17 No. 5, pp. 388-407.

Helle, A.J. (2005), "Security culture and risk management is a management responsibility", ISSN 0085-7130, available at: www.telenor.com/en/resources/images/Page_011-014_tcm28-45146.pdf (accessed May 11, 2013).

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Höne, K. and Eloff, J.H.P. (2002), "Information security policy: what do international information security standards say?", *Computers & Security*, Vol. 21 No. 5, pp. 402-409.

Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H. (2003), "An integrated system theory of information security management", *Information Management & Computer Security*, Vol. 11 No. 5, pp. 243-248.

Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H. (2006), "An empirical study of information security policy on information security elevation on Taiwan", *Information Management & Computer Security*, Vol. 14 No. 2, pp. 104-115.

Horrocks, I. (2001), "Security training: education for an emerging profession", *Computers & Security*, Vol. 20 No. 3, pp. 219-226.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-659.

Humphreys, E. (2008), "Information security management standards: compliance, governance and risk management", *Information Security Technical Report*, Vol. 13 No. 4, pp. 247-255.

ISO/IEC 17799:2000 (2000), "Information technology – code of practice for information security management", International Organization for Standardization (ISO) and theInternational Electrotechnical Commission (IEC), Geneva.

ISO/IEC 27000:2012 (2012), "Information technology – security techniques – information security management system – overview and vocabulary", International Organization for Standardization (ISO) and theInternational Electrotechnical Commission (IEC), Geneva.

ISO/IEC 27001:2005 (2005), "Information technology – security techniques – information security management systems – requirements", International Organization for Standardization (ISO) and theInternational Electrotechnical Commission (IEC), Geneva.

ISO/IEC 27002:2005 (2005), "Information technology – security techniques – code of practice for information security management", International Organization for Standardization (ISO) and theInternational Electrotechnical Commission (IEC), Geneva.

Jarvelainen, J. (2013), "IT incidents and business impacts: validating a framework for continuity management in information systems", *International Journal of Information Management*, Vol. 33 No. 3, pp. 583-590.

Kankanhalli, A., Teo, H.K., Tan, B.C.Y. and Wei, K.K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139-154.

Katsikas, S.K. (2000), "Healthcare management and information systems security: awareness, training or education?", *International Journal of Medical Informatics*, Vol. 60 No. 2, pp. 129-135.

Kevork, E.K. and Vrechopoulos, A.P. (2009), "CRM literature: conceptual and functional insights by keyword analysis", *Marketing Intelligence & Planning*, Vol. 27 No. 1, pp. 48-85.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2006a), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14 No. 1, pp. 24-36.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Morrow, D.W. (2006b), "The top information security issues facing organizations: what can government do to help?", *Information Systems security*, Vol. 15 No. 4, pp. 51-58.

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. 7, pp. 493-508.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25 No. 4, pp. 289-296.

Ma, Q., Johnston, A.C. and Pearson, J.M. (2008), "Information security management objectives and practices: a parsimonious framework", *Information Management & Computer Security*, Vol. 16 No. 3, pp. 251-270.

Ma, Q., Schmidth, M.B. and Pearson, J.M. (2009), "An integrated framework of information security management", *Review of Business*, Vol. 30 No. 1, pp. 58-69.

Martins, A. and Eloff, J.H.P. (2002), *Information Security Culture*, Security in the Information Society (IFIP/SEC2002), Kluwer Academic, Boston, MA.

Mitropoulos, S., Patsos, D. and Douligeris, C. (2006), "On incident handling and response: a state-of-the-art approach", *Computers & Security*, Vol. 25 No. 5, pp. 351-370.

Mouratidis, H., Jahankhani, H. and Nkhoma, M.Z. (2008), "Management versus security specialists: an empirical study on security related perceptions", *Information Management & Computer Security*, Vol. 16 No. 2, pp. 187-205.

Musa, A.A. (2010), "Information security governance in Saudi organizations: an empirical study", *Information Management & Computer Security*, Vol. 18 No. 4, pp. 226-276.

NIST (2003), *Building an Information Technology Security Awareness and Training Program (Special publication No. 800-850)*, National Institute of Standards and Technology, US Department of Commerce, Gaithersburg, Maryland.

NIST (2004), *Computer Security Incident Handling Guide (Special Publication No. 800-861)*, National Institute of Standards and Technology, US Department of Commerce, Gaithersburg, Maryland.

NIST (2011), *Glossary of Key Information Security Terms (IR No. 7298)*, National Institute of Standards and Technology, US Department of Commerce, Gaithersburg, Maryland.

Organisation for Economic Co-operation and Development (2002), "Guidelines for the security of information systems and networks: towards a culture of security", available at: www.oecd.org/sti/interneteconomy/15582260.pdf (accessed April 13, 2013).

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Hawaii, 3-6 January*.

Palmer, M.E., Robinson, C., Patilla, J.C. and Moser, E.P. (2001), "Information security policy framework: best practices for security policy in the e-commerce age", *Information Systems Security*, Vol. 10 No. 2, pp. 1-15.

Payment Card Industry – Data Security Standards (PCI – DSS) (2010), "Data security standard: self-assessment questionnaire C and attestation of compliance", available at: www.pcisecuritystandards.org/documents/pci_saq_c_v2.pdf (accessed May 20, 2013).

Peltier, T.R. (2005), "Implementing an information security awareness program", *Security Management Practices*, Vol. 14 No. 2, pp. 37-49.

Perks, C. and Beveridge, T. (2003), *Guide to Enterprise IT Architecture*, Springer-Verlag, New York, NY.

Posthumus, S. and von Solms, R. (2004), "A framework for the governance of information security", *Computers & Security*, Vol. 23 No. 8, pp. 638-646.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Rees, J., Bandyopadhyay, S. and Spafford, E.H. (2003), "Prires: a policy framework for information security", *Communications of the ACM*, Vol. 46 No. 7, pp. 101-106.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organizational security culture: extending the end-user perspective", *Computers & Security*, Vol. 26 No. 1, pp. 56-62.

Schultz, E. (2004), "Security training and awareness – fitting a square peg in a round hole", *Computers & Security*, Vol. 23 No. 1, pp. 1-2.

Siponen, M.T. (2001), "Five dimensions of information security awareness", *Computers and Society*, Vol. 31 No. 2, pp. 24-29.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Sundt, C. (2006), "Information security and the law", *Information Security Technical Report*, Vol. 11 No. 1, pp. 2-9.

Thomson, K.L., von Solms, R. and Louw, L. (2006), "Cultivating an organizational information security culture", *Computer Fraud & Security*, Vol. 2006 No. 10, pp. 7-11.

Thomson, M.E. and von Solms, R. (1998), "Information security awareness: educating your users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S. (2010), "A security standards' framework to facilitate best practices' awareness and conformity", *Information Management & Computer Security*, Vol. 18 No. 5, pp. 350-365.

Upfold, C.T. and Sewry, D.A. (2005), "An investigation of information security in small and medium enterprises (SMEs) in the EasternCape", *Proceedings of the ISSA-2005 New Knowledge Today Conference, Sandton, Johannesburg, June 29-July 1*.

Veiga, A.D. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, Vol. 29 No. 2, pp. 196-207.

Veiga, A.D., Martins, N. and Eloff, J.H.P. (2007), "Information security culture – validation of an assessment instrument", *Southern African Business Review*, Vol. 11 No. 1, pp. 147-166.

von Solms, B. (2000), "Information security – the third wave?", *Computers & Security*, Vol. 19 No. 7, pp. 615-620.

von Solms, B. (2001), "Corporate governance and information security", *Computers & Security*, Vol. 20 No. 3, pp. 215-218.

von Solms, B. (2006), "Information security – the fourth wave", *Computers & Security*, Vol. 25 No. 3, pp. 165-168.

von Solms, B. and von Solms, R. (2004), "The 10 deadly sins of information security management", *Computers & Security*, Vol. 23 No. 5, pp. 371-376.

von Solms, R. and von Solms, B. (2006), "Information security governance: a model based on the direct-control cycle", *Computers & Security*, Vol. 25 No. 6, pp. 408-412.

Vroom, C. and von Solms, R. (2004), "Towards information security behavioral compliance", *Computers & Security*, Vol. 23 No. 3, pp. 191-198.

Ward, P. and Smith, C.L. (2002), "The development of access control policies for information technology systems", *Computers & Security*, Vol. 21 No. 4, pp. 356-371.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009), "An integrated view of human, organizational, and technological challenges of IT security management", *Information Management & Computer Security*, Vol. 17 No. 1, pp. 4-19.

Wiant, T.L. (2005), "Information security policy's impact on reporting security incidents", *Computers & Security*, Vol. 24 No. 6, pp. 448-459.

Williams, P.A. and Saull, R. (2001), "Information security governance", *Information Security Technical Report*, Vol. 6 No. 3, pp. 60-70.

Williams, Z., Ponder, N. and Autry, C.W. (2009), "Supply chain security culture: measure development and validation", *The International Journal of Logistics Management*, Vol. 20 No. 2, pp. 243-260.

Wood, C.C. (1995), "A policy for sending secret information over communications networks", *Information Management & Computer Security*, Vol. 4 No. 3, pp. 18-19.

Yap, C.S., Soh, C.P.P. and Raman, K.S. (1992), "Information system success factors in small business", *Omega*, Vol. 20 No. 5, pp. 597-609.

About the authors

Abhishek Narain Singh is a Research Scholar in the Department of Management Studies, Indian Institute of Technology Delhi, India. He holds Masters and Bachelor Degree in Computer Science and Engineering. His current research interests includes information security management and e-governance. He has presented the research work at national and international fora. He has been a Fellow of Deutscher Akademischer Austausch Dienst and a Visiting Scholar to Ludwig-Maximilian-University, Munich in Germany. Abhishek Narain Singh is the corresponding author and can be contacted at: singhabhi444@gmail.com

M.P. Gupta is a Chair Professor of Information Systems & E-governance at the Department of Management Studies, Indian Institute of Technology Delhi, India. He has contributed significantly in the areas of e-commerce and e-governance. He has also authored/co-authored book "Government Online" and several papers that appeared in national and international

journals/conference proceedings. He founded the "International Conference on E-governance" (ICEG) in 2003 which is running into its tenth year. He is involved in several policy-making committees on ICT in the Center and State Governments in India. He is the recipient of the Best Professor Award in 2012 at Singapore and prestigious Humanities & Social Sciences (HSS) fellowship of Shastri Indo Canadian Institute, Calgary (Canada) and was a Visiting Fellow at the University of Manitoba in 1996.

Dr Amitabh Ojha is a Senior Civil Servant with Ministry of Railway, Government of India. He has had tenures as a Second Secretary at the High Commission of India, London and as a Director with Government of India, Ministry of Development of North Eastern Region, New Delhi. He holds Doctoral Degree from the Indian Institute of Technology Delhi, India. His research interests include e-government adoption, effect of e-government on citizens' trust in government agencies and administrative reforms through e-government. His research has published in various national and international journals.