The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Received 9 May 2013
Revised 12 November 2013
2 January 2014
Accepted 2 January 2014

Impact of information security initiatives on supply chain performance

An empirical investigation

Sindhuja P.N.
Department of IT and Operations, IBS Hyderabad, a Constituent of IFHE, Deemed to be University, Hyderabad, India

Abstract

Purpose – The purpose of this empirical research is to attempt to explore the effect of information security initiatives (ISI) on supply chain performance, considering various intra- and inter-organization information security aspects that are deemed to have an influence on supply chain operations and performance.

Design/methodology/approach – Based on extant information security management and supply chain security management literature, a conceptual model was developed and validated. A questionnaire survey instrument was developed and administered among supply chain managers to collect data. Data were collected from 197 organizations belonging to various sectors. The study used exploratory and confirmatory factor analysis for data analysis. Further, to test the hypotheses and to fit the theoretical model, structural equation modeling techniques were used.

Findings – Results of this study indicate that ISI, comprising technical, formal and informal security aspects in an intra- and inter-organizational environment, are positively associated with supply chain operations, which, in turn, positively affects supply chain performance.

Research limitations/implications – This study provides the foundation for future research in the management of information security in supply chains. Findings are expected to provide the communities of practice with better information security decision-making in a supply chain context, by clearly formulating technical, formal and informal information security policies for improving supply chain performance.

Originality/value – In today's global supply chain environment where competition prevails among supply chains, this research is relevant in terms of capability that an organization has to acquire for managing internal and external information security. In that sense, this study contributes to the body of knowledge with an empirical analysis of organizations' information security management initiatives as a blend of technical, formal and informal security aspects.

Keywords Information security, Empirical survey, Structural equation modeling, Supply chain operations, Supply chain performance

Paper type Research paper

Information Management & Computer Security
Vol. 22 No. 5, 2014
pp. 450-473

0968-5227
DOI 10.1108/IMCS-05-2013-0035

Introduction

During the post-industrial period since the early-1980s, there have been drastic changes in the business environment due to the unprecedented development of information systems. It has become all-pervasive in almost all the industries (Kankanhalli *et al.*, 2003; Chang and Ho, 2006; Knapp *et al.*, 2006; Werlinger *et al.*, 2009). Because organizations rely more and more on information systems to perform most of their business

operations, concerns about controlling and securing information has become paramount. One of the biggest challenges that today's businesses face is regarding the security of information arising from various sources and in varied forms. This threat to information security is a by-product of the unparalleled confidence and trust on information technology systems to realize the business goals. Increased organizational dependence on information systems has led to a proportional increase in the impact on the organization of compromised information security (Kankanhalli *et al.*, 2003). It was reported by the Ernst and Young Survey (2008) that a growing number of organizations have begun to understand the importance of information security and recognize the nexus between security and a strong brand and reputation. In addition, Brotby (2009) reported that nearly two-thirds of the breaches are underreported due to management's fear of adverse publicity and the fact that the size of losses may scare other stakeholders. In an inter-organizational or a supply chain perspective, the information that an organization exchanges with its trading partners is among the most important of its assets. This calls for secured communication and information sharing and demands the streamlining of information flows. In this context, information security is a critical issue that has attracted the attention of the communities of research and practice.

In the current business context, information security practices seem to have evolved from addressing trivial security violations to managing situations that are highly susceptible to security threats. It has also evolved from an information systems perspective to an organizational perspective with a broader focus and wider appeal (Brotby, 2009). Similarly, supply chain management is also witnessing a paradigm shift from competition to collaboration among organizations globally. Partly due to this, information security also seems to transcend the intra-organizational setting to be part of an inter-organizational setting. As supply chains are viewed as a network of interconnected technology systems, the information is subject to security risk at various points in the supply chain. This necessitates the need to examine the information security practices in the supply chain.

As observed by the communities of practice, global supply chains have to face many challenges that come with the trans-border transportation of goods and services and more businesses have recognized information security as a driver for business improvement (Ernst and Young Survey, 2008). As suggested in the literature, an effective supply chain information security lies in the coordination of people, processes and technology (Ashenden, 2008) and consideration of technical, formal and informal controls of the information system (Dhillon, 2007). As supply chain is considered to be both internal and external (Nadler and Kros, 2008), information security issues also need to be considered from internal, as well as external perspectives. Hence, the objective of this study is to examine the impact of information security initiatives (ISI) on supply chain operations from an intra- and inter-organizational perspective. The study has taken into account the information security dimensions along the three levels of information systems – technical, formal and informal – as suggested by Dhillon (2007), from an internal and external perspective of an organization. Further, the study will also examine the impact of security-enabled supply chain operations on supply chain performance.

Given the overarching importance of ISI in the supply chain, this research tried to provide a better understanding of the related issues in a systematic manner. The literature review explores past research in the area and identifies significant gaps that

prompted to frame relevant research questions. Based on the research questions a research model and associated hypotheses were developed. Further, the research methodology section details on questionnaire development using Q-sort methodology, data collection process and data analyses, using structural equation modeling techniques and interpretations thereafter. Finally, the manuscript discusses the expected managerial and theoretical implications of this study.

Literature review

Literature on security is widely spread across various streams like information systems, information technology, organizational security, supply chain security and information security. The following section briefly discusses a selection of previous studies relating to information security.

Information security – an organizational perspective

The concept of information security can be traced back to the origin of information itself and the fact that it needs to be protected was widely acknowledged by practitioners and researchers. Dlamini *et al.* (2009) discussed in detail the evolution of information security research. The authors pointed out evidence of information safety practices during the first century when Julius Caesar used secret codes to secure confidential information during the process of message transfer. Gradually, the practices of information security evolved from securing handwritten messages, telegrams and telephonic conversations to the advanced world of network computing. The focus of information security shifted from the basics of securing the secrecy of information to a much advanced accessibility policies and access control mechanisms. In addition, the information security practices have evolved from addressing minor breaches to managing those with huge impact on organizations' economic growth.

Although the technological solutions for security seem to be sophisticated and stringent, humans are the first level of protection to secure information assets (Chen *et al.*, 2008) and human factor is the weakest link in information security chain (Finne, 1996). Ashenden (2008) examined the challenges of information security from an organizational perspective, considering the extent of management and human challenges involved in information security management. Werlinger *et al.* (2009) presented a holistic view of the challenges faced by information technology (IT) practitioners in their organizations from human, organizational and technological perspectives. Human challenges identified were lack of security training, lack of security culture and communication of security issues. Organizational challenges included risk estimation, open environments and freedom, lack of budget, security as a secondary priority, tight schedules, business relationships with other organizations, distribution of IT responsibilities, access control to sensitive data, size of the organization and top management support. Technological challenges comprised of complexity of systems, vulnerabilities in systems and applications, mobile and distributed access and lack of efficient security tools.

Kankanhalli *et al.* (2003) developed an integrated model that proposed relationships among organizational factors, information system (IS) security practices and IS security effectiveness. The study categorized information security practices or measures as deterrents and preventives. A partial least square analysis of the data collected from 63

IS managers showed that organizational factors were significant and positive toward security measures.

Chang and Ho, (2006) examined the influence of organizational factors on the effectiveness of implementing the information security management standard, BS 7799-2 (1999), in various organizations in Taiwan. Their study revealed that the organizational factors positively influenced information security implementation. Kraemer and Carayon (2007) proposed a macro-ergonomic conceptual framework that provided a basis for understanding the linkages of human and organizational factors to human errors that contribute to computer and information security. Their study revealed that organizational issues of security culture and policy, communication failures, etc. are frequent causes of errors in the context of information security.

Ma *et al.* (2008) refined a set of information security objectives and practices extracted from previous studies and reports from academic world and practice. The complete set of ISO 17799 (ISO 27001:2005) security practices that covered 10 control areas were used to develop a questionnaire that measured the perceptions regarding ISM practices. Analysis of the data obtained from 354 certified information security professionals revealed that "confidentiality", "accountability", "integrity" and "availability" are the factors identified under information security objectives dimension and eight factors related to the 10 control areas of ISO 27001 were identified as the most common information security practices.

There is a high degree of consensus among many researchers that formulation and utilization of information security policy (ISP) is critical for effective information security management (Herath and Rao, 2009; Hong *et al.*, 2006; Fulford and Doherty, 2003; von Solms, 1998; Siponen, 2000). Bulgurcu *et al.* (2010) examined the antecedents of employee compliance with the organizational information security policy and the impact of information security awareness on an employee's attitude to comply with the ISP. The results revealed that an employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply and also ISA has a positive and significant influence on the attitude and beliefs. Guo *et al.* (2011) empirically investigated the factors influencing the attitudes and behaviors of end-users toward organizational information security. They developed and tested a non-malicious security violation model by analyzing the data gathered from end-users at workplace. The study suggested the need for aligning the business objectives with the security objectives, as well as linking of their job performance evaluation with the level of adherence to the IS security policies enforced.

The significance of information security awareness is widely accepted among information security researchers (Thomson and von Solms, 1998; Straub and Welke, 1998; Siponen, 2000). Hagen *et al.* (2008) discussed the implementation of organizational information security measures and assessed the effectiveness of such measures. Results showed that effectiveness of awareness creating activities was significant in organizations where security measures are implemented. Kritzinger and Smith (2008) proposed a conceptual model for information security retrieval and awareness (ISRA) to enhance the security awareness among all the IT authority levels and also assist IT authority levels in decision-making about information security processes. They proposed on developing a knowledge base for information security to ensure that the technical information security issues do not surpass the non-technical human-related

information security issues. They proposed a model that consisted of dimensions to measure ISRA, mechanisms for information security retrieval and awareness process, and mechanisms for measuring and monitoring them. Chen *et al.* (2008) conducted an inter-cultural study in the USA and Taiwan to investigate the relationship between security awareness learning exposure and performance in those security awareness outcomes. Results showed that users exposed to training showed greater performance and such programs can strengthen the people factor. Chang and Lin (2007) examined the influence of organizational culture on information security management effectiveness. Organizational culture characteristics were measured using two dimensions of culture, i.e. internal/external orientation and flexibility/control orientation. They found significant positive relationships between organizational culture and ISM. Asai and Perez (2012), in a cross-cultural study comparing the US, UK and Japanese cultures, observed that cultural differences could lead to unintentional information security breaches in cross-cultural environments. They found that countries that are more inclined toward their national culture faced more security problems than those countries with less cultural differences.

Dhillon (2007) classified information security as having three levels – technical, formal and informal. At the technical level, information security controls consists of defensive mechanisms such as firewalls, antivirus applications, voice analysis, digital signatures, biometric devices and other authentication protocols intended to protect the software applications, hardware and data that resides in computer systems. Formal controls are rule-based and dictate how technical controls are deployed and used to manage information security within the organization. Apart from these two controls, informal controls play a vital role in shaping up the security structure of an organization. Informal controls consist of training and awareness programs conducted to orient employee behavior related to information security.

Information security – a supply chain perspective

Sheffi (2001) observed that internal security efforts taken by one trading partner can be potentially annulled by the lack of security efforts taken by the other or lack of coordination between the trading partners. To ensure complete security, each organization in the supply chain has to use both internal and external security measures. Sarathy (2006) gave a conceptual understanding of the importance of supply chain security and the sources of internal and external risk. Voss *et al.* (2008) examined the extent to which the organizations use security initiatives, both internal and external. They observed that organizations considering security to be a strategic priority observed higher levels of security execution and better security performance and also showed a greater ability to recognize and recuperate from security incidents both within the organization and across the supply chain. Yang and Wei (2011) empirically identified the important dimensions of security management and their impacts on security performance in the shipping sector in Taiwan. The four important dimensions identified were facility and cargo management, accident prevention and processing, information management and partner relationship management. The study indicated that information management and partner relationship management were positive and significant with respect to security performance.

Supply chain operations

Supply chain operations encompass all activities associated with the flow of information and transformation of goods from raw materials through the final customer. Williams *et al.* (2009) investigated the drivers of supply chain security that impacted the supply chain operations. They argued that government, customer, society and competitors are the drivers of supply chain security. When it comes to supply chain security, the decisions to be made are not always easy; thus, managers will benefit from understanding the sources of the decisions related to supply chain operations. During late 1990s, a growing number of firms have shown interest in electronic commerce as an effective tool for business–business operations. Kalakota and Whinston (1997) observed that electronic commerce was used as a medium to effectively link customer demand information to upstream supply chain functions (e.g. manufacturing, distribution, and sourcing) and, subsequently, facilitated demand-driven supply chain operations. Russell and Saldanha (2003) brought forth five tenets of security-aware supply chain operations. Their views were based on a comprehensive review of supply chain disruptions across the globe such as terrorists' attacks, contingency planning efforts, etc. They suggested that healthy trading partner relationships, responsibility for the cross-border supply chain security, capability to accommodate unexpected delays and disasters, maintaining a suite of communication channels to manage crisis and being agile help in the management of supply chain operations in a secured manner.

For the purpose of this study, we define security-aware supply chain operations to contain supply chain information integration, supply chain robustness and supply chain operational decision-making.

Supply chain performance

Many studies can be found in the literature that deals with supply chain performance measurements (Gunasekaran *et al.*, 2001; Sambasivan *et al.*, 2009). Various researchers have attempted to measure supply chain performance in unique ways and developed a wide variety of performance measures. Kurien and Qureshi (2011) reviewed the supply chain performance literature in detail and evaluated the various types of performance measures used in supply chain models. The supply chain operations reference (SCOR) model, developed by the Supply Chain Council (Stewart, 1995), is the most commonly used tool among all the extant conceptualizations and frameworks developed for measuring supply chain performance. It provides a practical framework that takes into account the performance requirements of member organizations in a supply chain. In this model, supply chain activities are considered as a series of inter-organizational processes that are inter-linked, as well as possess a common process-oriented language for communication among supply chain members in the following decisions areas: plan, source, make and deliver. One of the views of the SCOR model is that a supply chain must be measured in multiple dimensions. Hence, each of the above decision areas is considered as an important intra-organizational process in the supply chain having five dimensions of measurement:

(1) supply chain reliability;
(2) responsiveness;
(3) flexibility;
(4) cost; and
(5) efficiency in asset utilization.

In agreement with Mentzer and Konrad (1991), the SCOR model describes supply chain performance as being efficient in terms of resource utilization and effective in terms of accomplishment of the supply chain objectives.

Based on the review of literature on information security, supply chain management, it was evident that there is a need for an integrated framework of information security that could enhance the performance of the supply chain. The next section clearly details the objectives of this research.

Research objectives

As evident from the above review, information security clearly encompasses information security standards, procedures and practices, culture, policy, awareness creation, various organizational factors, etc. from within and across organizations. A careful look at most of the studies in the area of information security (Kankanhalli *et al.*, 2003; Karyda *et al.*, 2005; Chang and Ho, 2006; Ma *et al.*, 2008; Werlinger *et al.*, 2009) makes it evident that a number of studies have been done within an organizational setting. However, most of the conceptual studies (Sarathy, 2006; Michelberger and Labodi, 2009; Voss *et al.*, 2008) suggested for extending the scope to consider the environment external to the organization, as in supply chain.

Most of the studies done in the area of information security focused on either technological controls or formal controls or informal controls (Dhillon, 2007). However, there is need for developing a comprehensive and integrated information security framework that incorporates all the three controls in a collective way, within and across organizations.

Many researchers have conceptually suggested the need for considering the internal and external dimensions of information security in organizations (Ashenden, 2008; Finne, 1996) in general and in global supply chain environment (Sarathy, 2006) in particular. However, the literature is void of empirical research that examines the internal and external initiatives that contain the above three controls, for information security management in supply chains. Literature is also seen silent on the studies examining the influence of ISI on either organizational performance or supply chain performance.

Based on these gaps, the following objectives were broadly developed:

- to develop a comprehensive information security framework that considers technical, environmental (internal and external) and management (formal and informal) aspects, from an organizational and inter-organizational perspective in a supply chain context; and
- to explore the potential outcome of information security measures on supply chain operations and in turn, the supply chain performance.

The next section would discuss the theoretical foundation based on which the comprehensive framework for information security of supply chains is developed.

Theoretical framework and hypotheses development

The theoretical support for the research framework is based on the Integrated System Theory of Information Security proposed by Hong *et al.* (2003), Resource Dependency Theory (RDT), proposed by Pfeffer and Salancik (1978), and Technology-Organization-Environment (TOE) Framework by Tornatzky and Fleischer (1990).

Hong *et al.* (2003) developed an integrated system theory of information security management (ISM) by analyzing five different theories related to information security. The theories are security policy theory (Gupta *et al.*, 2001), risk management theory (Wright, 1999), internal control and auditing theory (Wright, 1999; ISO/IEC 17799, 2000), management system theory (Schultz *et al.*, 2001) and contingency theory (Drazin and Van de Ven, 1985; Lee *et al.*, 1982).

The theory gave a comprehensive picture of information security and could be applied to predict the organizational attitudes and behavior toward information security management, as well as information security decision-making. Conclusions that can be derived out of this theory are:

- information security is an internal as well as an external function;
- information security functions are multidimensional and cross-functional; and
- information security deals with protecting information from all forms and sources of information.

RDT by Pfeffer and Salancik (1978) is based on the assumption that an organization's decisions and actions are influenced by its dependence on critical resources and those actions can be explained based on a particular dependency position. As observed by Ratnasingham and Kumar (2000), RDT is based on the following premises:

- external environment of the operating concern;
- internal environment that define the structure, policies, procedures, standards, etc. in an organization; and
- interactions among the trading partners for performing daily business transactions.

Extending the above premises to the current study, RDT could explain the organizational and inter-organizational environment and their interactions considering ISI as a critical resource. In this context, an organization's external environment is nothing but its supply chain environment. Information security policies, standards, procedures, practices, etc. form its internal environment. Further, it is imperative that the trading partners interact with each other for efficient functioning of the supply chain.

TOE framework by Tornatzky and Fleischer (1990) is based on the assumption that an organization, adopting and implementing any technological innovation, is influenced by technological, organizational and environmental context. In this study, the information security measures adopted by an organization can be considered as an innovative technological context, formal and informal structures, policies and communication processes related to information security can form the organizational (internal) context and technology support infrastructure of the trading partners can form the organization's external environment context.

Based on the above theoretical understanding and extending it to a supply chain context, this research tried to explore the multifaceted dimensions of information security practices from within and across organizations in a supply chain. The conceptual model for research has been developed based on the theoretical underpinnings and primarily attempted to capture the information security measures at an intra- and inter-organizational level, by consolidating the technical, formal

(organizational/managerial) and informal (people/social) controls under one roof, in a supply chain context. Borrowing from the incumbent ISM standards and practices in literature (Ma *et al.*, 2008; ISO 27001:2005), this research conceptualized internal and external information security dimensions to include the sub-constructs, namely, physical security, logical security, information security policy, information security culture and information communication.

Benefitting from the study of Russell and Saldanha (2003), the study has considered supply chain operations dimensions which include operational decision-making, supply chain robustness and supply chain information integration. This study used the framework developed by SCOR (Stephens, 2001; Stewart, 1995) for measuring supply chain performance, as it is found more relevant for the study. The conceptual model is represented in Figure 1.

Influence of ISI on supply chain operations

Various researchers (Rice and Caniato, 2003; Sarathy, 2006; Voss *et al.*, 2008) have conceptualized the importance of information security considerations on supply chain operations. According to Sarathy (2006), security-enabled supply chain operations yield benefits for the organization, as well as the supply chain. For instance, the use of radio frequency identification tags helps in monitoring the demand status, thereby enabling firms to adjust production schedules and quantities, procurement and channelize the finished products to the market at an optimum demand level. This has helped in achieving overall profitability, satisfy the customer and, more importantly, retain the customer.

Rice and Caniato (2003) observed that as organizations go in favor of sophisticated ISI, their focus shifts from industry standards, policies and government regulations to more collaborative events such as information integration, supply chain continuity

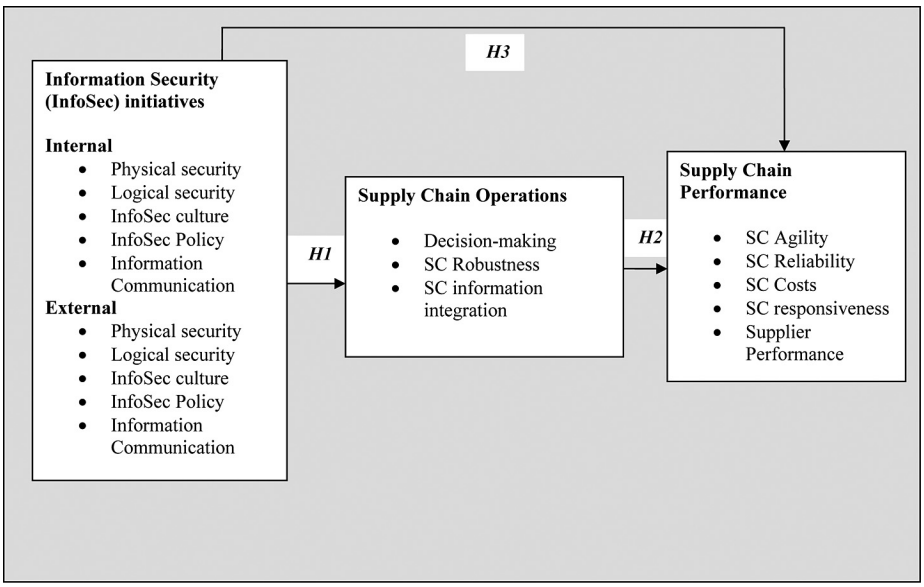

Figure 1.
The conceptual model

planning and decision-making. Sarathy (2006) pointed out that security-related supply chain interruption can have spilling effects on production schedules, inventory levels, manufacturing volume and product availability. He observed that security-related sources of risk occur at various points along the supply chain and information that is being transferred is one such point of risk. Voss *et al.* (2008) posited that to ensure complete security of all supply chain operations, all organizations in the supply chain must provide for internal, as well as external ISI.

Based on the above arguments, it is hypothesized that:

H1. ISI have a positive influence on supply chain operations.

Influence of supply chain operations on supply chain performance

Earlier in the literature review section, we defined supply chain operations to include operational decision-making, robustness and information integration. Zhou *et al.* (2007) examined the integration of supply chain practices and information sharing for supply chain management. Supply chain practices considered were supply chain planning aspects, just-in-time production aspects and delivery practices. The survey instrument based on seven-point Likert scale measured the respondents' perception regarding the supply chain practices in their organizations. Usable data ($n = 125$ firms) were collected from senior executives. Data were analyzed using regression analysis to examine the impact of supply chain practices (independent variable) on delivery performance (dependent variable). Results revealed that effective supply chain practice improved the supply chain delivery performance.

Sezen (2008) empirically examined the impact of information sharing and supply chain integration on supply chain performance. Questionnaire, anchored on a five-point Likert scale was administered in Turkish manufacturing firms. Data collected from 125 firms was analyzed using factor analysis to extract factors that measured supply chain performance and supply chain integration. Results of regression analyses revealed that SC information sharing and integration influenced the performance of the supply chain significantly.

According to Lee *et al.* (1982), information integration across the supply chain is indispensable to avoid problems such as excessive stock, disorder of capacity planning, inefficient shipping, incorrect production scheduling, poor customer service quality, etc. Yu *et al.* (2010) observed that information sharing is vital to improve the performance of the supply chain.

Sarathy (2006) posited that a secure, robust and resilient supply chain is capable of enhancing the overall supply chain performance. Russell and Saldanha (2003) suggested that the companies should search for new tenets of supply chain operations such as building capabilities for disaster management, contingency planning, etc. to improve the performance of the supply chain.

Based on the above evidences and arguments, it is hypothesized that:

H2. Supply chain operations have a positive influence on SC performance.

Direct influence of ISI on supply chain performance

As mentioned by Sarathy (2006), reliability and performance of a supply chain depends on accurate supply chain information. Therefore, physical security (safe storage rooms, fire alarms, etc.) and logical security (antivirus solutions, biometric methods, etc) are

widely used in organizations. These security initiatives are deployed to prevent unauthorized access to data and premises. Ultimately, the goal is to prevent alteration of the cargo details while in transit. It also helps in protecting the confidentiality of supply chain information. He also stated that information security measures can also promote supply chain intelligence. It deals with maintaining a log for tracking the authorities who have access to containers at various points along the supply chain. Voss *et al.* (2008) suggested that internal and external security initiatives will improve the overall performance of the supply chain. Owing to above discussions and arguments and to examine the direct influence of information security on supply chain performance, it is hypothesized that:

H3. ISI have a positive influence on SC performance.

Research methodology

Unit of analysis

Most of the past empirical studies on information security have considered organization as the unit of analysis. As this study looked into the intra- and inter-organizational factors influencing ISI and its influence on supply chain operations and performance, this study also considered organization as the unit of analysis. To capture the effect of the entire supply chain activities (both upstream and downstream), this research is specifically set in a different context, by focusing on organizations at the middle tiers (focal firms, tier-1 and tier-2) of the supply chain, assuming those organizations to have knowledge of both upstream and downstream activities.

Questionnaire development

Measurement items used in this study were either developed from literature or adopted from previous studies. Identification and validation of newly generated items were done in two stages:

(1) item generation through literature review; and

(2) pilot testing using Q-sort methodology.

In the first stage, potential items were generated through an extensive literature review which helped in identifying the content domain of the major constructs. This also helped in the generation of initial items and the definition of the constructs. The initial pool of items was reviewed by academic and industry experts.

During the second phase, the items were pilot-tested using Q-sort methodology (Nahm *et al.*, 2002). The pool of items was subjected to three sorting rounds to ensure that each item was placed under the right constructs. To confirm the content validity of the scale, different practitioners were asked to sort the items into various construct categories. At the end of third round, the Q-sort method was terminated as the raw agreement score of 0.93, Cohen's Kappa of 0.928 (Cohen, 1960), and the average placement ratio of 0.93 were considered as an excellent score of inter-judge agreement, indicating a high level of reliability and construct validity (Nahm *et al.*, 2002). A total of 91 items were developed for the three constructs internal information security, external information security and supply chain operations, categorized into 16 sub-constructs, using Q-sort method. The items for supply chain performance construct were taken from previous studies. The final questionnaire used for the survey is given in the Appendix.

Survey administration and sample demographics

According to Kotulic and Clark (2004), a survey eliciting information related to organizational information security and supply chain issues will be successful only if the researcher has a good rapport with employees of the organization. Going by their terms, an expanding network methodology was used to collect the data relevant for this research. The expanding network methodology was partially or fully used by various researchers (Malhotra *et al.*, 2005) in supply chain studies. In this method, a focal organization that has a good rapport with the researcher may give the contact list of their tier1 and tier-2 suppliers. In the current research, this expanding network method helped in getting the contacts of relevant suppliers. A web-based online version of the questionnaire was developed for the respondents identified through the expanding network methodology. The final survey questionnaire anchored on a 5-point Likert scale (ranging from 1– Strongly Disagree to 5 – Strongly Agree) was administered among supply chain functional managers of organizations belonging to various sectors. At the end of the survey, 197 responses were found to be useful for further analysis. Among the 197 respondents, 31 per cent belonged to pharmaceutical sector, 22 per cent from retail sector and remaining fall under various other sectors in small proportions. More than 70 per cent of the organizations rely on electronic transactions between their trading partners, and 65 per cent of the organizations had employee size above 1,000.

Data analyses, results and discussion

Based on 197 responses, all the constructs were tested for reliability, unidimensionality, convergent and divergent validity. Exploratory factor analysis was performed using the statistical software SPSS 16.0. Measurement and structural model was developed and tested using AMOS.

ISI construct has two dimensions: internal ISI and external ISI. To ensure divergent validity, a construct-level exploratory factor analysis (EFA) was done. Results are shown in Table I. All factor loading scores were above 0.7 (Hair and Anderson, 1995). Three factors emerged, namely; Internal Information Security Initiatives (IISI), External Information Security Access Controls (EISAC) and External Information Security Culture, Policy and Communication (EISCPC).

Factor names	Factor loadings Factor 1	Factor 2	Factor 3
IISI	0.912		
	0.841		
	0.912		
	0.849		
	0.879		
EISAC		0.794	
		0.835	
EISCPC			0.705
			0.868
			0.898
			0.803
Cumulative % of variance	35.4	62.7	83.02

Table I. Results of construct level factor analysis for ISI

A Cronbach's alpha score of 0.91 indicated a high reliability. To ensure unidimensionality, a confirmatory factor analysis (CFA) was done. Results are shown in Table II. The values indicated a good model fit.

To examine whether the three sub-constructs (IISI, EISAC and EISCPC) underlie the single second-order construct ISI, T-coefficient (Doll *et al.*, 1995) was calculated. The value of T-coefficient was found to be 0.95, indicating the existence of the single second-order construct ISI.

The *Supply Chain Operations* (SCO) construct was initially designed to have three dimensions: supply chain operational decision-making (SCODM), supply chain robustness and supply chain information integration (SCII). After factor analysis, a four-factor solution emerged. They were named as SCODM, supply chain continuity planning (SCCP), supply chain disaster recovery (SCDR) and SCII. Results of construct-level factor analysis are given in Table III.

A Cronbach's alpha score of 0.856 indicated a high reliability. To ensure unidimensionality, a CFA was done. Results are shown in Table IV. The values indicated a good model fit.

To examine whether the four sub-constructs (SCODM, SCCP, SCDR and SCII) underlie, the single second-order construct SCO, T-coefficient was calculated. The value

Table II.
Model fit indices for the first-order constructs of ISI

Sub-construct	Chi-Square (df)	Chi-Square/df	GFI	AGFI	NFI	RMSR
IISI	3.637 (4)	0.909	0.992	0.972	0.991	0.007
EISAC	2.931 (4)	0.733	0.994	0.978	0.970	0.012
EISCPC	9.351 (5)	1.870	0.981	0.942	0.931	0.022

Table III.
Results of construct-level analysis of SCO

	Factor loadings			
Factor names	Factor 1	Factor 2	Factor 3	Factor 4
SCODM	0.734			
	0.743			
	0.610			
	0.657			
	0.745			
	0.675			
SCCP		0.829		
		0.851		
		0.653		
SCDR			0.843	
			0.758	
			0.782	
SCII				0.688
				0.736
				0.780
				0.751
Cumulative % of variance	19.46	36.59	51.05	64.54

Notes: KMO measure of sampling adequacy = 0.727; Cronbach's alpha = 0.856

of T-coefficient was found to be 0.98, indicating the existence of a single second-order construct SCO.

All the 20 items of the *Supply Chain Performance* (SCP) construct were subjected to a construct-level EFA to examine discriminant validity. A five-factor solution having factor loadings above 0.6 emerged, and the factors accounted for 64.87 per cent of the total variance. The factors were named as supply chain agility (SCA), supply chain reliability (SCRel), supply chain costs (SCC), supply chain responsiveness (SCRes) and supplier performance (SP). Kaiser–Meyer–Olkin measure of sampling adequacy was 0.784. The reliability score of the dimension was 0.887. Results are presented in Table V. To examine unidimensionality of each sub-construct in SCP construct, CFA was performed. Table VI presents the model fit indices. It is evident from the table that all the indices indicated a good model fit and ensured unidimensionality.

To examine whether the five sub-constructs (SCA, SCRel, SCCosts, SCRes and SP) underlie the single second-order construct SCP, T-coefficient was calculated. The value

Sub-construct	Chi-Square/df	GFI	AGFI	NFI	RMSR
SCODM	2.98	0.960	0.908	0.934	0.016
SCCP	1.38	0.989	0.958	0.981	0.016
SCDR	1.180	0.991	0.965	0.981	0.013
SCII	2.02	0.990	0.948	0.981	0.006

Table IV.
Model fit indices for the first-order constructs of SCO

	Factor loadings				
Factor names	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
Supply chain agility	0.797				
	0.701				
	0.720				
	0.633				
	0.741				
	0.610				
Supply chain reliability		0.726			
		0.799			
		0.803			
		0.710			
Supply chain costs			0.781		
			0.824		
			0.659		
			0.621		
Supply chain responsiveness				0.831	
				0.673	
				0.740	
Supplier performance					0.601
					0.777
					0.788
Cumulative % of variance	17.69	31.91	43.88	54.66	64.87

Notes: KMO measure of sampling adequacy = 0.784; Cronbach's alpha = 0.887

Table V.
Results of construct-level analysis of SCP

of T-coefficient was found to be 0.97, indicating the existence of a single second order construct.

Results and discussion of structural model and hypotheses testing

After the measurement model, structural model was developed and structural equation modeling techniques (SEM) were used to test the hypotheses. The structural model of the research framework is presented in Figure 2. The model fit measures for the model are: GFI = 0.869, AGFI = 0.824, NFI = 0.846, CFI = 0.915, RMSR = 0.02 and RMSEA = 0.072. GFI and AGFI values were found to be above the acceptable value of 0.8. RMSR was found to be below the recommended value of 0.05. RMSEA was also found to be below the recommended value of 0.08. These fit indices indicated a good fit of the model to the data.

Although ISI were conceptualized as IISI and external information security initiatives, later during data analysis, both internal and external information security initiatives were found to underlie a single second order construct which was named as ISI. Hence the structural model given below considered ISI as a second order construct.

From the SEM analysis, out of the three hypothesized relationships, two were found to be significant using one-tailed tests. They include *H1* (impact of ISI on SCO) and *H2* (impact of SCO on SCP). The direct impact of ISI on SCP (*H3*) was found to be insignificant. The results of the SEM are presented in Table VII. The results indicated that ISI adopted by an organization has a positive influence on its supply chain activities, leading to better performance of the supply chain.

From the results, *H1* was found to be positive and significant ($\beta = 0.22$, $t = 2.49$) at $p < 0.01$. This result indicated that information security practices had an influence on an organization's supply chain operations such as decision-making, continuity planning, disaster recovery, information integration, etc. Information security practices included effective physical and logical access controls, good cultural climate, training and awareness, well-documented security policies and open communication channels. As observed by Dhillon (2007), good information security practices will take care of the

Sub-construct	Chi-Square/df	GFI	AGFI	NFI	RMSR
SCA	1.768	0.977	0.941	0.970	0.012
SCRel	3.3	0.966	0.898	0.946	0.012
SCCosts	3.02	0.985	0.927	0.968	0.006
SCRes	2.36	0.974	0.903	0.950	0.016
SP	1.26	0.990	0.962	0971	0.009

Table VI.
Model fit indices for the first-order constructs of SCP

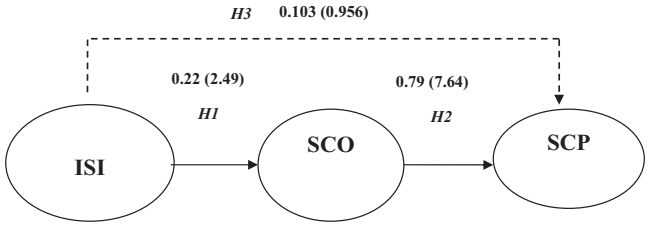

Figure 2.
Structural model

technological, organizational and human challenges faced by an organization. In corroboration with Dhillon's observation, this result indicated that information security practices can also take care of the above challenges, even at an inter-organizational level (as in supply chains). Thus, this result can be used to evaluate the effect of information security practices on supply chain activities at an inter-organizational level.

Results of *H2* were also found to be significant ($\beta = 0.769$, $t = 7.204$) at $p < 0.001$. This result is in corroboration with an earlier study by Li *et al.* (2005) where the author concluded that better supply chain management (SCM) practices lead to better supply chain performance. In addition, this result empirically confirms the fact that a secured and well-managed supply chain directly leads to enhanced supply chain performance. Earlier studies (Narasimhan and Jayaram, 1998; Tan *et al.*, 2002) had associated SCM performance directly to organizational performance. However, this result can be used to evaluate the inter-organizational (supply chain) performance.

Results of *H3* was found to be insignificant ($\beta = 0.095$, $t = 1.223$). This indicated that ISIs directly cannot impact the performance of a supply chain. There are other deciding factors such as supply chain operations, trading partner relationship, etc. that can act as a facilitator for enhanced supply chain performance. Another rationale for this finding may be attributed to the fact that ISIs are only a part of the solution for effective implementation of supply chain operations leading to improved supply chain performance.

The study identified important dimensions of information security practices that an organization can adopt to evaluate their security posture. Many organizations have a misguided belief that information security is all about technical security (Dhillon, 2007; Brotby, 2009). However, there are other elements of security at formal and informal levels which organizations give less importance. Moreover, organizations consider security only after a disaster occurs. This research forms a foundation to evaluate all levels of information security in a comprehensive manner. This included taking into account the human (informal), technological and organizational (formal) challenges that an organization may encounter at times of security violations and disasters. From the findings, it is suggested to have a parameter to measure all aspects related to security in an organization in a supply chain. This included the aspects related to physical security, logical security, culture, policy, awareness, personnel security, enforcement and disciplinary actions, etc. Although these aspects are stated by ISO standards for information security, they are rarely evaluated from a behavioral perspective. The scale developed for information security can be used by the organization to evaluate their security status at all levels.

This study provided a theoretical framework that consisted of various dimensions of information security and supply chain operations. Information security consisted of

Hypothesis	Relationship	Path coefficient	*t*-value	*p*-value	Results
H1	ISI → SCO	0.222	2.492	0.013**	Supported
H2	SCO → SCP	0.791	7.643	***	Supported
H3	ISI → SCP	0.103	0.956	0.452	Not Supported

Notes: Significant at: ***$p < 0.001$; **$p < 0.01$; CMIN/DF = 2.004; GFI = 0.869; AGFI = 0.824; NFI = 0.846; CFI = 0.915; RMSR = 0.02

Table VII.
Results of structural model

dimensions such as physical and logical security, information security culture, information security policies and information security awareness and information communication. Supply chain operations were defined to possess dimensions such as operational decision-making, supply chain continuity planning, disaster recovery and information integration. To this end, this study has contributed to the research community by providing a foundation for future research in this area.

Information security as a separate discipline was discussed from an organizational (internal) as well as inter-organizational (external) perspective. Although conceptualized earlier by various researchers, this is the first study of its kind to test and validate the concepts. The study was able to develop reliable and valid constructs based on theory and made use of it in developing and testing causal relationships. In this way, all the newly developed constructs can act as building blocks for future research.

Future scope, summary and conclusion

Although the current research made significant contributions for communities of research and practice, it has some limitations. Small sample size may be considered as a limitation of this study. Larger sample size may yield more valid results. Respondents of this study had varying levels of knowledge about information security practices and supply chain. These differences in their experience and years worked in the current organization were not considered during the data analysis. These variables may have an impact on their perception of information security practices in the supply chain. Organization size, level of investment on IT, organization structure, technical complexity, etc. may have an impact on the relationships defined in this study. These variables were not considered in this study. This study considered only original equipment manufacturer (OEM), tier 1 and tier 2 members of the supply chain. Considering the peripheral tiers may impact on the relationships developed in the current study.

In future, the study can be extended to analyze the industry-specific differences while implementing information security practices. Hence, the study may be conducted in each industry to arrive at more robust results. Such a study will benefit individual industries in implementing good security practices in the supply chain. This study examined the supply chain information security practices at an inter-organizational level. A supply chain-level study is also recommended for future exploration provided adequate number of supply chains can be identified to meet the methodological requirements. Such a study may take into account the supply chain-specific differences that may be vital while implementing information security practices in supply chains.

Although the study tried to consider the supply-and-demand side at the same level, most of the survey responses were from the supply side. Therefore, another study can be done exclusively to examine the buyer's (demand-side) opinion on information security practices in a supply chain. As buyer's perception of information security practices may differ from that of supplier's and may have an influence on information security practices.

In summary, future research can test the causal relationships for various industries, tiers, countries, supply chains, etc. provided adequate data could be collected for each case. This may help researchers to identify tier-, industry-, country- and network-specific causal relationships in the model. Contextual variables such as organization size, organization structure, level of IT complexity, etc. can be included in future studies to examine their influence and interactions in the implementation of information

security practices across organizations. This study may be extended to include variables such as supply chain tiers, supply chain structure, etc. to examine their influence and interactions on ISI.

Information security in supply chain is not a cost of doing business but an essential element of supply chain efficiency and effectiveness (Sarathy, 2006). Essentially, a business cannot likely compromise on the information security issues. Therefore, it is imperative that an organization gives due consideration to the information security aspects, especially as it affects the supply chain of which the organization is a part. This study has contributed to the communities of research and practice by developing and testing an integrated information security framework that considers intra- and inter-organizational activities and processes to strengthen the supply chain. In addition, it tried to give a more detailed understanding of the internal and external dimensions of ISI, affecting the supply chain operations and performance.

It is expected that the above contributions will benefit not only the academic community but also the information security practitioners and supply chain managers in designing cost-effective security mechanisms, developing a pervasive security culture and to consider information security management as an organizational issue, rather than a mere technical control. This empirical research aims at providing a better understanding of the information security objectives and practices, considering other organizational factors, for an effective information security management across the supply chain.

References

Asai, T.T. and Perez, J.L.C. (2012), "Human-related problems in information security faced by Japanese, British and American overseas companies because of cultural differences", *China-USA Business Review*, Vol. 11 No. 1, pp. 86-101.

Ashenden, D. (2008), "Information security management: a human challenge", *Information Security Technical Report*, Vol. 13 No. 4, pp. 195-201.

Brotby, W.K. (2009), *Information Security Management Metrics*, CRC Press, Boca Raton, FL.

BS 7799-2 (1999), *Information Security Management Part 2: Specification for Information Security Management Systems*, British Standards Institute, London.

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

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

Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008), "A cross-cultural investigation of situational information security awareness programs", *Information Management and Computer Security*, Vol. 16 No. 4, pp. 360-376.

Cohen, J. (1960), "A coefficient of agreement for nominal scales", *Educational and Psychological Measurement*, Vol. 20 No. 1, pp. 37-46.

Dhillon, G. (2007), *Principles of Information Systems Security: Text and Cases*, John Wiley and Sons, New York, NY.

Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M. (2009), "Information security: the moving target", *Computers and Security*, Vol. 28 Nos 3/4, pp. 189-198.

Doll, W.J., Raghunathan, T., Lim, S.J. and Gupta, Y.P. (1995), "A confirmatory factor analysis of the user information satisfaction instrument", *Information Systems Research*, Vol. 6 No. 2, pp. 177-188.

Drazin, R. and Van de Ven, A.H. (1985), "Alternative forms of fit in contingency theory", *Administrative Science Quarterly*, Vol. 30 No. 4, pp. 514-539.

Ernst and Young Survey (2008), *Global Information Security Survey 2008*, Ernst and Young LLP, London.

Finne, T. (1996), "The information security chain in a company", *Computers and Security*, Vol. 15 No. 4, pp. 297-316.

Fulford, H. and Doherty, N.F. (2003), "The application of information security policies in large UK-based organizations: an exploratory investigation", *Information Management and Computer Security*, Vol. 11 No. 3, pp. 106-114.

Gunasekaran, A., Patel, C. and McGaughey, R.E. (2001), "A framework for supply chain performance measurement", *International Journal of Production Economics*, Vol. 87 No. 3, pp-333-347.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), "Understanding nonmalicious security violations in the workplace: a composite behavior model", *Journal of Management Information Systems*, Vol. 28 No. 2, pp. 203-236.

Gupta, M., Chaturvedi, A.R., Metha, S. and Valeri, L. (2001), "The experimental analysis of information security management issues for online financial services", *ICIS 2000, Brisbane*, pp. 667-675.

Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management and Computer Security*, Vol. 16 No. 4, pp. 377-397.

Hair, J.F. and Anderson, R.E. (1995), *Multivariate Data Analysis*, Prentice Hall, Upper Saddle River, NJ.

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, pp. 154-165.

Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H. (2003), "An integrated system theory of information security management", *Information Management and 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 in Taiwan", *Information Management and Computer Security*, Vol. 14 No. 2, pp. 104-115.

Kalakota, R. and Whinston, A.B. (1997), *Electronic Commerce: A Manager's Guide*, Addison-Wesley Longman, Reading, MA.

Kankanhalli, A., Teo, H.-H., Tan, B.C. 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.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005), "Information systems security policies: a contextual perspective", *Computers and Security*, Vol. 24, pp. 246-260.

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

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies?", *Information and Management*, Vol. 41 No. 5, pp. 597-407.

Kraemer, S. and Carayon, P. (2007), "Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists", *Applied Ergonomics*, Vol. 38 No. 2, pp. 143-154.

Kritzinger, E. and Smith, E. (2008), "Information security management: an information security retrieval and awareness model for industry", *Computers and Security*, Vol. 27 Nos 5/6, pp. 224-231.

Kurien, G.P. and Qureshi, M.N. (2011), "Study of performance measurement practices in supply chain management", *International Journal of Business, Management and Social Sciences*, Vol. 2 No. 4, pp. 19-34.

Lee, S.M., Luthans, F. and Olson, D.L. (1982), "A management science approach to contingency models of organizational structure", *Academy of Management Journal*, Vol. 25 No. 3, pp. 553-566.

Li, S., Rao, S.S., Ragu-Nathan, T.S. and Ragu-Nathan, B. (2005), "Development and validation of a measurement instrument for studying supply chain management practices", *Journal of Operations Management*, Vol. 23.

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

Malhotra, A., Gosain, S. and El Sawy, O.A. (2005), "Absorptive capacity configurations in supply chains: gearing for partner-enabled market knowledge creation", *MIS Quarterly*, Vol. 29 No. 1, pp. 145-187.

Mentzer, J.T. and Konrad, B.P. (1991), "An efficiency/effectiveness approach to logistics performance analysis", *Journal of Business Logistics*, Vol. 12 No. 1, pp. 33-61.

Michelberger, P. and Labodi, C. (2009), "Development of information security management system at the members of the supply chain", *Annals of the University of Petrosani, Economics*, Vol. 9 No. 4, pp. 69-78.

Nadler, S.S. and Kros, J.F. (2008), "An introduction to Sarbanes-Oxley and its impact on supply chain management", *Journal of Business Logistics*, Vol. 29 No. 1, pp. 241-255.

Nahm, A.Y., Solis-Galvan, L.E., Rao, S.S. and Ragu-Nathan, T.S. (2002), "The Q-sort method: assessing reliability and construct validity of questionnaire items at a pre-testing stage", *Journal of Modern Applied Statistical Methods*, Vol. 1 No. 1, pp. 114-125.

Narasimhan, R. and Jayaram, J. (1998), "Causal linkage in supply chain management: an exploratory study of North American manufacturing firms", *Decision Science*, Vol. 9 No. 3, pp. 579-605.

Pfeffer, J. and Salancik, G.R. (1978), *The External Control of Organizations: A Resource Dependence Perspective*, Harper and Row, New York, NY.

Ratnasingham, P. and Kumar, K. (2000), "Trading partner trust in electronic commerce participation", in *Proceedings of the Twenty First International Conference on Information Systems*, Association for Information Systems, Atlanta, GA.

Rice, J. and Caniato, F. (2003), "Building a secure and resilient supply network", *Supply chain management review*, Vol. 7 No. 5, pp. 22-30.

Russell, D.M. and Saldanha, J.P. (2003), "Five tenets of security-aware logistics and supply chain operation", *Transportation Journal*, Vol. 42 No. 4, pp. 44-54.

Sambasivan, M., Nandan, T. and Mohame, Z.A. (2009), "Consolidation of performance measures in a supply chain environment", *Journal of Enterprise Information Management*, Vol. 22 No. 6, pp. 660-689.

Sarathy, R. (2006), "Security and the global supply chain", *Transportation Journal*, Vol. 45 No. 4, pp. 29-52.

Schultz, E.E., Proctor, R.W. and Lien, M.C. (2001), "Usability and security: an appraisal of usability issues in information security methods", *Computer and Security*, Vol. 20 No. 4, pp. 331-339.

Sezen, B. (2008), "Relative effects of design, integration and information sharing on supply chain performance", *Supply Chain Management: An International Journal*, Vol. 13 No. 3, pp. 233-240.

Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism", *International Journal of Logistics Management*, Vol. 12 No. 2, pp. 1-11.

Siponen, M.T. (2000), "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8 No. 1, pp. 31-41.

Stephens, S. (2001), "The supply chain council and the supply chain operations reference (SCOR) model: integrating processes, performance measurements, technology and best practice", *Annals of the Logistic Spectrum*, Vol. 34, pp. 16-18.

Stewart, G. (1995), "Supply chain performance benchmarking study reveals keys to supply chain excellence", *Logistics Information Management*, Vol. 8 No. 2, pp. 38-44.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision-making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-469.

Tan, F.B. and Hunter, M.G. (2002), "The repertory grid technique: a method for the study of cognition in information systems", *MIS Quarterly*, Vol. 26 No. 1, pp. 39-57.

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

Tornatzky, L.G. and Fleischer, M. (1990), *The Processes of Technological Innovation*, Lexington Books, Lexington, MA.

Von Solms, R. (1998), "Information security management: why information security is so important", *Information Management and Computer Security*, Vol. 6 No. 5, pp. 224-225.

Voss, M.D., Whipple, J.M. and Closs, D.J. (2008), "The role of strategic security: internal and external security measures with security performance implications", *Transportation Journal*, Vol. 28 No. 2, pp. 5-23.

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

Williams, Z., Leug, E.J., Taylor, R.D. and Cook, R.L. (2009), "Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS)", *International Journal of Physical Distribution and Logistics Management*, Vol. 39 No. 7, pp. 595-618.

Wright, M. (1999), "Third generation risk management practices", *Computers and Security*, Vol. 1 No. 2, pp. 9-12.

Yang, C. and Wei, H. (2011), "The effect of supply chain security management on security performance in container shipping operations", *Supply Chain Management: An International Journal*, Vol. 18 No. 1, pp. 74-85.

Yu, M., Ting, S. and Chen, C. (2010), "Evaluating the cross-efficiency of information sharing in supply chains", *Expert Systems with Applications*, Vol. 37 No. 4, pp. 2891-2897.

Zhou, H. and Bentor, W.C. Jr (2007), "Supply chain practice and information sharing", *Journal of Operations Management*, Vol. 25 No. 6, pp. 1348-1365.

Further reading

Autry, C.W. and Bobbit, L.M. (2008), "Supply chain security orientation: conceptual development and a proposed framework", *The International Journal of Logistics Management*, Vol. 19 No. 1, pp. 42-64.

Da Veiga, A. and Eloff, J.H.P. (2009), "A framework and assessment instrument for information security culture", *Computers and Security*, Vol. 29 No. 2 pp. 1-12.

Da Veiga, A., 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.

Dhillon, G. (2001), "Violation of safeguards by trusted personnel and understanding related information security concerns", *Computers and Security*, Vol. 20 No. 2, pp. 165-172.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: toward socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Dhillon, G. and Torkzadeh, G. (2006), "Value focused assessment of information system security in organizations", *Information Systems Journal*, Vol. 16 No. 3, pp. 293-314.

Fiala, P. (2005), "Information sharing in supply chains", *Omega*, Vol. 33 No. 5, pp. 419-423.

Gay, L.R. and Airasian, P. (2003), *Educational Research: Competencies for Analysis and Applications*, Merrill/Prentice Hall, Upper Saddle River, NJ.

Green, K.W. Jr., Whitten, D. and Inman, R.A. (2008), "The impact of logistics performance on organizational performance in a supply chain context", *Supply Chain Management*, Vol. 13 No. 4, pp. 317-327.

Russell, D. and Gangemi, G.T. (1991), *Computer Security Basics*, O'Reilly and Associates, Sebastopol, CA.

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

Siponen, M.T. and Oinas-Kukkonen, H. (2007), "A review of information security issues and respective research contributions", *The Database for Advances in Information Systems*, Vol. 38 No. 1, pp. 60-81.

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

Von Solms, R. (1996), "Information security management: the second generation", *Computers and Security*, Vol. 15 No. 4, pp. 281-288.

Appendix. Questionnaire

Internal information security

Our organization has proper technical/logical access controls (password mechanisms, data, backup and network security, anti-virus solutions, etc) to protect its information assets from unauthorized access, use, disclosure, disruption, modification or destruction.

Our organization has proper physical controls (protection of physical facilities, data storage centers and premises from unauthorized entry, environmental dangers, etc).

Our organization maintains a good information security cultural climate (attitudes, beliefs, norms, assumptions, awareness and training programs, etc).

Information security policies and procedures are consistently enforced (policy statements, policy enforcement, personnel security, etc)in our organization.

We believe that internal communication of information is vital (inter-departmental communication and information sharing).

External information security

Our trading partners have enforced proper physical controls (protection of physical facilities, data storage centers and premises from unauthorized entry, environmental dangers, etc).

Our trading partners have enforced proper logical access controls (password mechanisms, data, backup and network security, anti-virus solutions, etc) to protect its information assets from unauthorized access, use, disclosure, disruption, modification or destruction.

We have well-documented policies and procedures for ensuring secured flow of information with our trading partners.

We and our trading partners try to maintain a good information security cultural climate that fosters smooth functioning of the supply chain.

We and our trading partners feel that proper communication of information is vital to the success and continuity of supply chain activities.

We keep each other informed of the events that may affect the other party.

About the supply chain operations in your firm

Operational decision-making

Our supply chain information enables to make decisions in logistics.

Our supply chain information enables to make decisions in production/manufacturing.

Our supply chain information enables to make decisions in inventory management.

Our supply chain information enables to make decisions in shipping.

Our supply chain information enables to make decisions in material handling.

Our supply chain information enables to make decisions in purchasing/procurement.

Accurate information is usually available for decision making.

Supply chain robustness

Our organization has documented the measures to be taken when an emergency or disaster occurs, covering crisis communications, business process and it resources recovery.

Our organization has a written disaster recovery plan for systems, data and telecommunications.

Our organization has a regular and auditable maintenance schedule for all of the business continuity plan components.

Our organization would return to normal operations in short order, if a serious security breach were to happen.

Our organization would not have problem with supply chain operations in the event of a significant security breach in the supply chain.

Our organization has procedures that ensures speedy resumption of essential operations following system failure/interruption.

Supply chain information integration

Information integration with trading partners in the supply chain is important.

Our organization effectively collaborates with trading partners to maintain information symmetry along the supply chain.

There is a high level of integration of information across the supply chain.

There is a high level of communication and coordination between all functions across the supply chain.

About the performance of your supply chain

Supply chain agility

Our supply chain is able to respond to changes in market demand without overstocks or lost sales.
Our supply chain is able to leverage the competencies of our partners to respond to market.
Our supply chain is able to forecast market demand.
Our supply chain has reduced in-bound lead-times.
Our supply chain ensures non-value added time reduction in the pipeline.
Our supply chain ensures that processes are streamlined throughout the supply chain.

Supply chain reliability

Our supply chain system increases our order fill rate.
Our supply chain system increases our inventory turns.
Our supply chain system reduces our safety stocks.
Our supply chain system reduces our inventory obsolesces.

Supplier performance

We receive timely delivery of materials/components/products from our partners.
We receive speedy delivery from our partners.
We receive quality delivery from our partners.

Supply chain costs

Our supply chain system reduces inbound and outbound costs.
Our supply chain system reduces warehousing costs.
Our supply chain system reduces inventory-holding cost.
Our supply chain system reduces our product warranty claims.

Supply chain responsiveness

Our supply chain has short order fulfillment lead times.
Our supply chain has short order-to-delivery cycle time.
Our supply chain has fast customer response time.

About the author

Sindhuja P.N. is an Assistant Professor at IBS Hyderabad, a Constituent of IFHE, Deemed to be University. She received her PhD in Management with IT as specialization from ICFAI University Dehradun, India. Her doctoral work has focused on information security aspects in supply chain. Her research has been presented in various international conferences. Her doctoral thesis was awarded first prize at the Ninth AIMS International Conference on Management in 2012. She is a member of Indian-Subcontinent Decision Sciences Institute. Sindhuja P.N. can be contacted at: sindhuja.menon@ibsindia.org