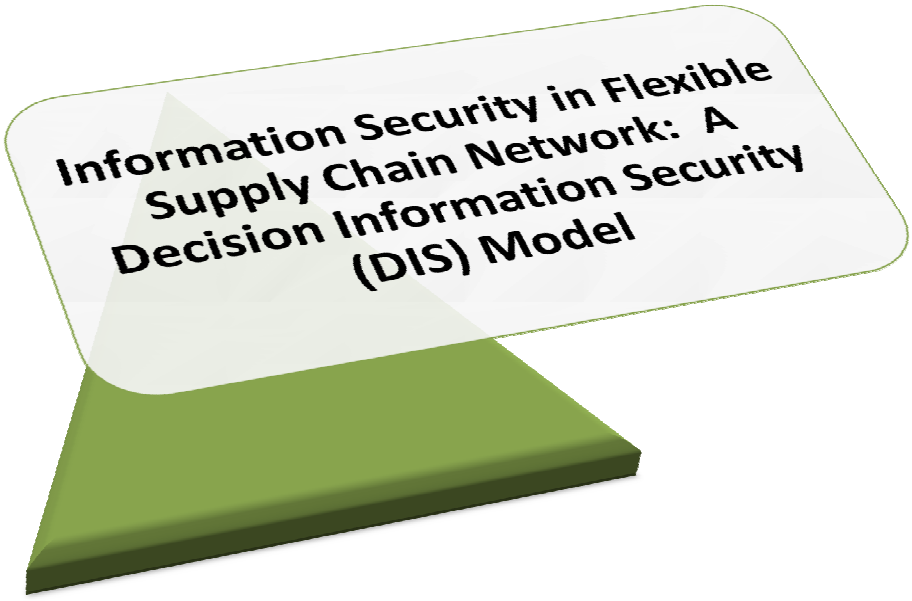


Prof. Subhash Wadhwa
Professor, Indian Institute of Technology-Delhi, India
swadhwa@mech.iitd.ernet.in

Anuj Prakash
Research scholar, Department of Mechanical Engineering, IIT Delhi India
anujpra@gmail.com

Prof. S. G. Deshmukh
Director, ABVIITM, Gwalior & Professor, IIT, Delhi, IIIT,Delhi, India
deshmukh@mech.iitd.ernet.in

Bharat Wadhwa
Project Associate (ACSS), Indian Institute of Technology-Delhi, India
wadhwa_bharat @hotmail.com

ABSTRACT

• The Internet, with its unprecedented growth, is a promising platform to exchange information along the business channels. The purpose of this study was to determine the factors that are critical to organizations in their adoption decision of Information Systems (IS). Security assurance across flexible supply chain network is a critical factor for international business managers and in the evolution of international trade generally. A security system for a flexible supply chain network is progressing as a network security management in an existing security solution foundation. In this paper, it is tried to design a security solution structure for enhancing the internal security. This study proposed the structure of Decision Information Security (DIS) in order to build a supply chain network security management system which also have the inherent properties of the security systems e.g. confidentiality, authentication, availability. This paper suggests the needs for security mechanism capabilities that will allow private and public sector groups involved in global trade to effectively mitigate the threat of IT and loss of competitiveness.

KEYWORDS

- *Information System*
- *Security System*
- *Information Security Systems (ISS),*
- *Flexible Supply chain Network*
- *Internet*

Introduction

This In today's business environment, most organizations are facing significant pressure to make their operational, tactical, and strategic processes more efficient and effective. Information technology (IT) has become an attractive means of improving these processes. Consequently, organizations have implemented several strategies to improve effectiveness and to enhance efficiencies through the use of IT. Until recently, the main focus of many organizations was on improving internal operations. However, establishing strategic alliances between trading partners along the supply chain with full flexibility through the utilization of IT may result in great benefits. At the same time, there is a threat of the information security also due to the computer crimes.

However, most IS security managers pay more attention to technical issues and solutions such as firewalls, routers, and intrusion detection software, while pay less focus on soft issues such as the hazards caused by end users' lack of IS security awareness (Katz, 2005). Information security awareness can be described as a state where users in an organization are aware of their security mission (Siponen, 2000). It can be distinguished two categories of security awareness: framework and content (Siponen, 2000). The former concerns standardization, certification and measurement activities, whereas the latter addresses the human and socio-cultural aspects of information security awareness. Furthermore, Puhakainen (2006) points out that 59 IS security awareness approaches have been put forward by practitioners and scholars. These approaches can be classified into two categories. Studies in the first category consider IS security awareness to mean attracting users' attention to IS security issues (e.g., Hansche, 2001; Katsikas, 2000). Studies in the second category regard IS security awareness as users' understanding of IS security and, optimally, committing to it.

IS security awareness plays a significant role in the process of the overall information security of any organization (Thomson and von Solms, 1998; Straub and Welke, 1998). The important role of the human factor in IS security has been recognized by both the research community and IS security practitioners (Parker, 1998, 1999; Siponen, 2000,

2001). As such, users' IS security awareness is reflected in their attitudinal and behavioural patterns (Beatson, 1991; Lafleur, 1992; Gaunt, 1998, 2000; Ho¨ne and Eloff, 2002; Mitnick, 2002; Puhakainen, 2006).

In the present paper, the soft issues along with some technical issues have been taken into the consideration. To make the quick and safe decision in supply chain, a model of the Decision Information Security (DIS) has been developed and proposed in the present work. This system provides the inherent facility of the internet with a role based security mechanism for a flexible supply chain network.

The remainder of the paper has been arranged in the following manner: the literature review has been presented in section 2 and section 3 presents the flexibility in supply chain. The generic view of the information security has been presented in section 4. The proposed DIS model has been delineated in section 5. In section 6, the paper has been concluded.

2. Literature Review

There have been in recent years increased information security considerations in organizations (Straub and Welke, 1998; Schlienger and Teufel, 2003). This is mainly due to the fact that information systems and the Internet are today used not only by organizations to increase their competitiveness, but also by criminals. Based on recent studies (Whitman and Mattord, 2005), staff errors are rated among the top threats to information assets in organizations. It is essential to convince IS security staff of the imperative need to enforce information security measures (Pfleeger and Pfleeger, 2003). Cybertrust (2005) argues that the problem of information security is two-fold: firstly it is due to the increase in economic and political uncertainty and secondly to the pressure from customers and players of the network. In fact, a single case of abuse can cause more costs than the establishment of a security system (Czernowalow, 2005). Enforcing security awareness through education and training is hence paramount. It is essential to ensure that all users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work (BS7799, 1999). However, slowly but surely information security is getting into the forefront of things, and has been promoted from a by-product to an integral part of business operations (Conner and Coviello, 2004).

3. Flexibility in Supply Chain Management

A generalized model of a supply chain presented in figure 1 shows four levels in a supply chain. As a second player, the manufacturer produces the final product(s). The left most level is assumed to be the highest level while the rightmost is the lowest level in the supply chain. There may be any number of suppliers directly above the manufacturer. These suppliers may have their suppliers and the chain could extend to any number of tiers. At each tier some sort of value addition and/or physical transformation of goods take place. On the downward side of the manufacturer(s) is the level whose function is to supply the finished products to the retailers (distribution).

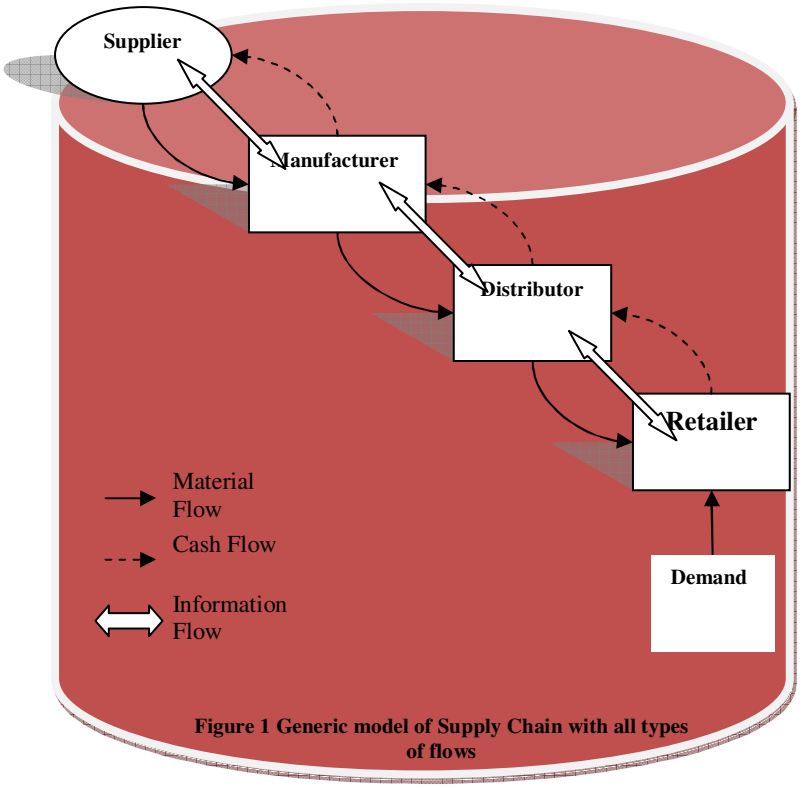


Figure 1 Generic model of Supply Chain with all types of flows

There are generally three kinds of flows along any two nodes of the supply chain as shown in: *material flow*, *information flow* and *cash flow*. The information flows from higher to lower echelons is generally

includes information regarding the quantity and the quality of the goods required (purchase order, etc.).
Flexibility as a generic notion is well known in several domains. The objective was to identify the performance of SC_s in dynamic and flexible environment. Garavelli (2003) views the supply chain flexibility and compares the results with no flexibility, partial flexibility, and full flexibility (figure 2). Wadhwa and Rao (2004) propose a unified framework for understanding flexibility in manufacturing system as well as supply chains. The framework is based on the key elements and basic constructs for analyzing their interaction for possible flexibility type. The framework is found to be useful as it could be applied to deal with the dynamic environment of SC_s. Similarly, Gunasekaran (2004) view supply chain flexibility as a way of providing options to the customers. Wadhwa and Rao (2003) examined the concept of flexibility in relation to the other important concept of agility and highlighted certain commonalities and differences and also suggested a possible vision for future evolution of these two important concepts. Therefore, it is necessary to deal dynamically with the information security to avoid problems in smooth running of supply chain. This is vital for SC_s to reduce overall cost with increased security. We have developed an information security system for flexible SC_s. In our model, we have shown only a single supplier, manufacturer, distributor and retailer and this model will work on the role base but in the case of FSCs, there will be a separate key of each node of the FSC.

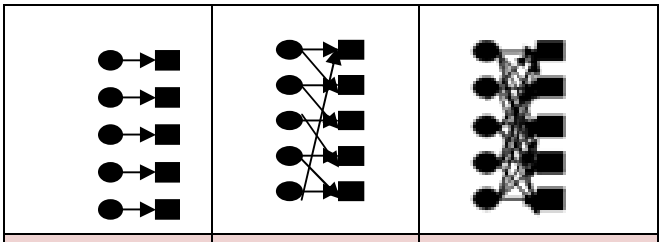


Figure 2: Supply Chains and Its Flexible Configuration based on Routing

4. Information System Security

4.1 Concepts

Information security is a broad subject that requires an adapted definition. The literature refers to both ''computer security'' and ''information systems security'', as these two concepts seem to be used interchangeably. According to (Ross, 1999), computer security can be defined in terms of domains, functions, and/or concepts. In terms of concepts, computer security can be categorized into confidentiality, integrity, authentication, access control, non-repudiation, availability, and privacy. In this context information security can also be defined as preserving confidentiality, protecting information from unauthorized use, assuring integrity and accuracy, and making data available to authorized users on a timely basis (Updegrove and Wishon, 2003).
In general, the principal reasons for providing IS security may include protection of resources, maintaining management control, ensuring safety and integrity, implementing policies and laws, and attaining operational advantages and economies (Turn, 1986). The expected outcomes of the effective information security system are as follows:

- Reduction on risk and potential impact on business strategies
- Value delivery through the optimization of investments
- Efficient utilization of resources
- Dynamic performance measurement
- Real time monitoring the operation in a supply chain to meet the business objectives

4.2 Supply Chain Management perspective

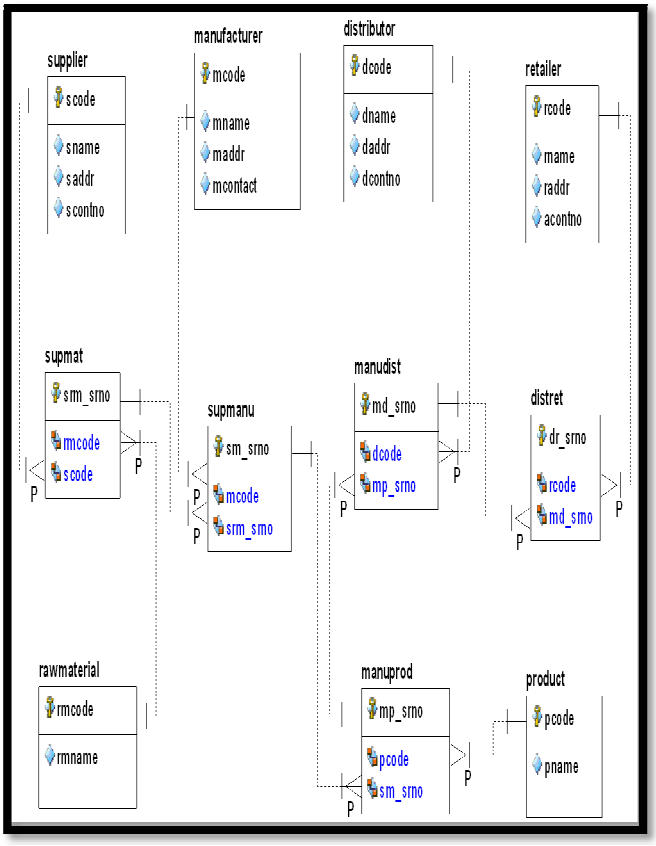
The vulnerability of any flexible supply chain is increasing with the advent of electronic commerce and open network architectures (Barsanti, 1999). Better computer literacy, increased computer user sophistication, and availability of advanced software tools may also contribute to increased IS security abuses in the future. Hence, management needs to pay more attention to IS security issues (Dhillon and Backhouse, 2000; Kankanhalli et al., 2003). Management attention for IS security has been low compared to other IS issues (Brancheau et al., 1996; Olnes, 1994). In a global information security survey of midsize and large firms, less than 50% of the 459 CIOs and IT directors polled said they had IT security awareness and training programs for employees (Verton, 2002). As highlighted in Kankanhalli et al. (2003), previous studies on IS security have focused on software for detecting IS security abuses (Straub and Nance, 1988), measures for preventing IS security abuses (Straub, 1990), perceptions of IS security adequacy

(Goodhue and Straub, 1991), and IS security planning models for management decision-making (Straub and Welke, 1998). For decision making problems, an ISS framework has been developed in supply chain which is described in the next section.

5. Decision Information Security (DIS) Model for Flexible Supply Chain

In the flexible supply chain framework, DIS will work among suppliers, manufacturers, distributors and retailers with its inherent facility of the confidentiality, integrity, availability and authentication. In such a framework, none of the players can be acquainted with the other players' capabilities or strategies. To develop such a model, the aim is to set a supply chain among all the players in such a manner that no one would be able to know the decision made by any member, which is not required by them. The proposed framework has been shown in figure 3. The detailed description of working of the proposed model has been described below.

In the propsed model of ISS, the leftmost echelon (supplier) is shown by the primary key know as *scode* and it includes the supplier name, address, and identification number (*sname, saddr, scountno*). The decision made by the suppliers can be shown by using these keys and the decision made by suppliers can be hid from the retailers by using the same key. Whereas raw material is identified by the primary key known as *rmcode*. The *rmcode* depicts the name of raw material delivered by the suppliers. The *supmat* table contains the data related to supplier (*scode*) and raw material (*rmcode*) i.e. which supplier is supply which raw material and each record is identified with a unique primary key *srm_srno*. The next player of supply chain (manufacturer) can use the primary key *mcode* for providing their information. It also shows the information regarding the name, address, identification number of manufacturers. In the *supmanu* table, the data is recorded associated with supplier, raw material and manufacturer i.e. a unique primary key *sm_srno* will offer the information of raw material provided by suppliers to the manufacturers. Thus *supmanu* table will be full of three data: *sm_srno* as unique key value for each record, *mcode* , and *srm_srno*. The data related to manufacturer, raw material and finished product is giving in the table known as *manuprod* and operated by *mp_srno*, a primary key. Product details are available in table product with uniquely identified key *pcode*. The role of the distributor can be played by using the primary key known as *dcode* and he can generate its demand to the manufacturer. Now the *manudist* table contains the data related to manufacturer, product and distributor and each record of distribution is identified with a unique primary key *md_srno*. The distributor is distributing which product to which retailer and each record is identified in the *distret* table with a unique primary key *dr_srno*. Retailer details are available in table retailer with uniquely identified key *rcode*. Here retailer can produce their demands. In the proposed framework, the decisions are saved in *supmat, supmanu, manudist,* and *distret* to show the decision made by suppliers, manufacturers, distributor and retailer. So they can secure their decisions information from any restricted member of the chain.



6. Conclusion

With the development of information society, the Internet based information system has brought convenience and pleasure to human life, but it is also misused by malicious or curious people to harm others and such side effects keep increasing. The present study analyzed the internet based flexible supply chain network development process and

direction of security systems. In addition, we proposed a structure of Decision Information Security (DIS) model, which is the most fundamental goal of a security system, has been proposed. The proposed model restricts to know the decision of the entire member for any particular strategy. Thus they can maintain the confidentiality and privacy also. Simultaneously, they can provide the decision information to the right member at the right time. The structure is applicable to any security policies in building supply chain network security management systems. This security system provides some inherent properties e.g. confidentiality, integrity, availability and authentication etc. As a future scope, it is necessary to develop intrusion cut-off methods that distribute traffic so that the processing of a large quantity of data does not slow down the network speed.

References

1. Barsanti C., (1999) Modern network complexity needs comprehensive security. *Security*, 36(7), 65–8.
2. Beatson JG., (1991) Security – a personnel issue. The importance of personnel attitudes and security education. In: Dittrich K, Rautakivi S, Saari J, editors. *Computer security and information integrity*. Amsterdam: Elsevier Science Publishers, 29–38.
3. Brancheau JC, Janz BD, Wetherbe JC., (1996) Key issues in information systems management: 1994–95 *SIM Delphi results. MIS Quarterly*,20(2), 225–42.
4. BS7799., (1999) *Code of practice for information security management.* UK: British Standards Institute.
5. Conner FW, Coviello AW, (2004), Information security governance: a call to action, *Corporate Governance Task Force Report of 2004*,
6. Cybertrust, Justifying security spending: how to make a business case for information security Available online at: (http://www.cybertrust.com/media/white_papers/cybertrust_wp_security_spending.pdf) (2005) [accessed 13.08.07].
7. Czernowalow M. *Lack of policy causes IT risks*. Available from: ITWEB, <http://www.itweb.co.za> [accessed 15.07.05].
8. Dhillon G, Backhouse J., (2000) Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125–8.
9. Garavelli. (2003), Flexibility configurations for the supply chain management, Int. J. Prod. Economics; 85, 141-153
10. Gaunt N., (1998) Installing an appropriate IS security policy in hospitals. *Int. Journal of Medical Informatics*, 49(1), 131–4.
11. Gaunt N., (2000) Practical approaches to creating a security culture. *Int. Journal of Medical Informatics*, 60(2), 151–7.
12. Goodhue DL, Straub DW., (1991) Security concerns of system users: a study of perceptions of the adequacy of security. *Information and Management*, 20(1), 13–27.
13. Gunasekaran A. Patel C. McGaughey R., (2004) A framework for supply chain performance measurement; Int. J. Production Economics; 87: 333–347
14. Hansche S. (2001) Designing a security awareness program: part I. *Information System Security,* 10(1), 14–22.
15. Hone K, Eloff JHP., (2002) What makes an effective information security policy? *Network Security*, 6, 14–6.
16. Kankanhalli A, Teo HK, Tan BCY, Wei KK., (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139–54.
17. Katsikas SK., (2000) Health care management and information system security: awareness, training or education? *International Journal of Medical Informatics*, 60(2), 29–35.
18. Katz, FH., (2005) The effect of a university information security survey on instructing methods in information security. *In: Proceedings of the second annual conference on information security curriculum development*; 43–8.
19. Lafleur LM., (1992) Training as part of a security awareness program. *Computer Control Quarterly*, 10(4), 4–11.

20. Mitnick KD., (2002) *The art of deception: controlling the human element of security*. USA: Wiley Publishing.
21. Olnes J., (1994) Development of security policies. *Computers and Security*, 13(8), 628–36.
22. Parker DB., (1998) *Fighting computer crime: a new framework for protecting information.* USA: John Wiley & Sons.
23. Parker DB., (1999) Security motivation, the mother of all controls, must precede awareness. *Comp. Security J.*, 15(4), 15–23.
24. Pfleeger CP, Pfleeger SL., (2003) *Security in computing*. 3rd ed. Prentice Hall.
25. Puhakainen P, (2006) *A design theory for information security awareness*. PhD thesis, University of Oulu.
26. Ross ST., (1999) *Unix systems security tools.* The McGraw-Hill Companies, 444. ISBN-10: 0079137881;
27. Schlienger T, Teufel S., (2003) Information security culture – from analysis to change. *SA Computer Journal*, 31, 46–52.
28. Siponen MT., (2000) A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41.
29. Siponen MT., (2001) Five dimensions of information security awareness. *Computers and Society*, 31(2), 24–9.
30. Straub DW, Nance WD., (1988) Uncovering and disciplining computer abuse: organizational responses and options. *Information Age*, ISSN: 0261-4103, 10(3), 151–6.
31. Wadhwa, S., Rao, K. S., (2003), Enterprise Modeling of Supply Chains involving multiple entities flows: Role of Flexibility in Enhancing Lead Time Performance, *SIC Journal*; 12 (1):5-20
32. Wadhwa, S., Rao, K.S. (2004) A Unified Framework for Manufacturing and Supply Chain Flexibility, *Global Journal of Flexible Systems Management*; 5(1):15-22