ISSN: 1839 - 0846

Design E-SCM Information Security Framework

Maryam Mahdikhani (Corresponding author)
m.mehdikhani290@yahoo.com
E-MBA and member of young researcher's society, Shahid Bahonar University, Kerman, Iran

Asadolah Khahande Karnama
Assistant Professor, Shahid Bahonar University, Kerman, Iran

Milad Beirami
M.A.student of Public Adminastration, Islamic Azad University, Rafsanjan, Iran

ABSTRACT

Electronic Business (e-Business) is revolutionizing the way of communication between Internal and external stakeholders in an organization. E-business can lead to competitive advantage and at the same time, increase profitability. There are several factors resulting on the success of e-business. One of the most important factors is Security. It is thus clear that information technology (IT) and the emerging e-business application and related to security are gaining a pivotal role in managing supply chain. This paper examines the impact of E-business on supply chain on information security aspect among other types of supply chains. The current paper reviews security and supply chain literatures and then investigates framework of information technology in supply chain management. Areas of supply chain which need security attention are then proposed in e-supply chain information security framework and this will be considered as a guideline for managers to find out if their e-supply chain network is secure enough. Through the paper, one realizes that Information Security in every information based-system will be vital.

Keywords: *E-business; E-Supply chain Management; business Security*

1. INTRODUCTION

Over the last years enterprises and individuals have started to conduct business over computer networks, especially the Internet. This development is commonly summarized as electronic business (e-business). Electronic Business which is commonly referred to as e-business, which is the utilization of information and communication technology (ICT) in conduct business on the internet, not only buying and selling but also servicing customers and collaborating with business partner. Electronic business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers (Velmurugan, 2009). Information security is one key component of national security. Many experts believe that under normal circumstances, the so-called information security refers to the state of the social informatization in one country and the country's information technology system being free from external threats and invasion (Luo yixin, 2011). Therefore, Security is the key to the success of e-business and lack of security is the significant problem on the way to e-business success. During every business transaction, the parties involved should feel security with the people and the companies. It must be established and managed continuously in business transaction activities (Velmurugan, 2009). It is not difficult to see that information security mainly includes three aspects, i.e. human security, physical security and safe operation. Human security mainly refers to the safety awareness, legal awareness, safety skills and so on of computer users; physical security refers to the measures and processes in the protection of computer equipment, facilities (including network) and other media from natural and man-made destruction. It involves security of environment, equipment and media; safe operation mainly includes risk management of systems, audit tracking, backup and recovery, emergency and so on (Luo yixin, 2011).

2. LITERATURE REVIEW

2.1. Supply Chain Management and Electronic Supply Chain

Supply chain is the integration of key business process from end user through original suppliers that provides products, services, and information that add value for customers and other stakeholders. Supply

ISSN: 1839 - 0846

chain management means coordinating, scheduling and controlling procurement, production, inventories and deliveries of products and services to customers (Yeung et al, 2009). In the context of increasingly globalized and competitive economy where organizations are part of an environment characterized by networks of inter- and intra-organizational relationships, an important prerequisite of information sharing emerges as supply chain integration (SCI) (Ipek Koçoglua et al,2011). Correct supply chain relationships based on strategic collaboration with supply chain partners (Simchi et al,2003) as a result of SCI, leverage the flow of timely, accurate and quality information (Li S et al,2006).

However, although the definitions in the literature regarding SCI encompass the complementarities between integration and information sharing, in the means that SCI supports effective and efficient flow of information (Gaile et al,2006), therefore IT and respective e-business tools and methods are more importantly viewed as having a role in supporting the collaboration and coordination of supply chains through information sharing. Objectives of e-business in supply chain management are to provide information availability and visibility, enable single point-of contact of data, allow decisions based on total supply chain information, and enable collaboration with supply chain partners. Efficiency of information transfer, information availability and transparency of relevant business information are only a few of the benefits provided by e-business solutions to support supply chain integration. A supply chain is called an e-supply chain when it is electronically managed, typically with web-based software.

Improvements in supply chains regularly bring an attempt to make information flow automatically (Poirier et al, 2000). The need of flexibility and adoptability in a dynamic e-business environment which focuses on network integration has introduced electronic supply chain management (E-SCM). E-SCM refers to "the supply chain that is built via electronic linkages and structurally based on technology-enabled relationships" (Williams, L.R et al, 2002).

E-SCM includes order treatment, organizing production, stock management, match delivery and transportation management, inventory management, customer service and payment management.

1) ***Order treatment.*** Order treatment is to identify and manage the attainable orders. When orders come, enterprises must identify which can be done and then analyze the cost and benefit according to the production capability. In this way, e-SCM reduces the error and cycle-time, and improves the efficiency.
2) ***Organizing production.*** Organizing production improves the communication among suppliers, enterprises and customers, and removes the difficulties of production management. To some extent, E-SCM makes the forecast of sales more accurate and organizes the production efficiently.
3) ***Stock management.*** Stock management is to smooth the flow of information between enterprises and their suppliers. By using e-commerce, enterprises gather information about the sales and future demand, and offer it to their suppliers. At the same time, enterprises get the price list and the catalog of the products from their suppliers. On the other hand, managing their stock through the internet, enterprises make the products' range of stock wider and reduce the number of stock personnel.
4) ***Match delivery and transportation management.*** In match delivery, enterprises can integrate the total supply chain by monitoring the consignments in the match delivery center, and tracing the transportation of the goods. In transportation, enterprises can exert their effects on optimizing resources, reducing transportation cost, tracing the cargo and delivering them to the right place timely.
5) ***Inventory management.*** Through e-commerce system, enterprises can communicate with each other about the inventory, such as the information of orders delayed and stock status. This can reduce the inventory cost and enhance the efficient utilization of their warehouses.
6) ***Customer service.*** Through internet, to receive and adjust the complaints from customers will be more convenient. It reduces the cost of informing customers of the necessary replacement or repairing.
7) ***Payment management.*** With the development of the technology and the security management of the internet, enterprises can settle accounts with their trade partners and customers on line (Closs, D.J et al, 2004).

2.2. Definition of Electronic Business

In order to be able to define an approach to e-business security, a working definition of e-business is needed. The definition of the term used here is based on a review of a number of basic concepts essential to an understanding of the business environment in general, and in particular the changes it has gone through in recent year. E-Business is a platform for communications and information sharing between business to business or business to consumers, which enables the streamlining of business processes involved in Supply Chain, and may facilitate efficient, effective performance improvement in Supply Chain Management (Asanka Hiroshana ,2007).The e-business involves the automation of all the business processes in value

ISSN: 1839 - 0846

chain-form procurement or purchasing of raw materials, to stock holding, distribution and logistics, to sales and marketing, after sales, invoicing, debt, collection and more. E-business includes models and methods of doing business, as well as all processes of business. E-business could be described in the following way:
EB ≡ f (EC, CRM, SCM, RP, BI, etc.)
Where: EB – E-business;
EC – E-commerce;
CRM – Customer Relationship management;
SCM – Supply Chain Management;
RPM – Resource Planning;
BI – Business inelegance.

2.3. Concept of business security

E-business is a powerful tool for business transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customers as well as for suppliers and employees. However, implementing the e-business applications that provide these benefits may be impossible without a coherent, consistent approach to e-business security. Traditional network security has focused solely on keeping intruders out using tools such as firewalls. This is no longer adequate. E-business means letting business partners and customers into the network, essentially through the firewall, but in a selective and controlled way, so that they access only the applications they need. To date, organizations have controlled and managed access to resources by building authorization and authentication into each e-business application. E-business security is an overarching business issue that, based on analyzed risks, establishes the threat acceptance and reduction parameters for the safe use of technology. As an overarching issue, e-business security can be thought of as being absolutely fundamental to the effective and efficient use of information technology (IT) in support of e-business.

E-business depends on providing customers, partners, and employees with access to information, in a way that is controlled and secure. Managing e-business security is a multifaceted challenge and requires the coordination of business policy and practice with appropriate technology. In addition to deploying standards bases, flexible and interoperable systems, the technology must provide assurance of the security provided in the products.

As technology matures and secure e-business systems are deployed, companies will be better positioned to manage the risks associated with disintermediation of data access. Through this process businesses will enhance their competitive edge while also working to protect critical business infrastructures from malefactors like hackers, disgruntled employees, criminals and corporate spies.Figure 1 presents a particularly approach to e-business in terms of security: how these main components presented interact and the main frame in which they change information (Flynn BB et al,2010). The architecture contains components that cannot be omitted components that interact for assuring the process called as SCM, supply chain management.

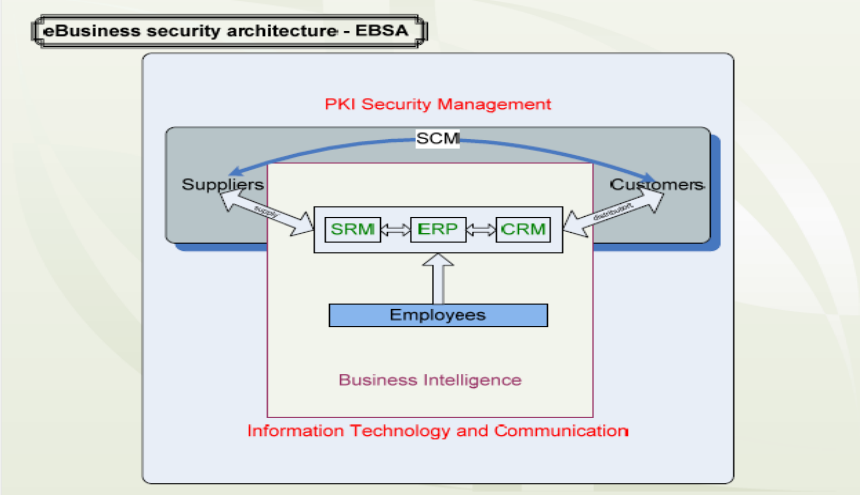

Figure1; EBSA, e-business security architecture

The components on which the presented architecture is based on are, (Flynn BB et al,2010):

ISSN: 1839 - 0846

Applications for Customer Relationship Management, CRM, used for interacting between various departments such as sales, marketing and client services; the main aspects of these applications is client orientation, trying to provide the best services to customers and collecting feed-back for interested departments;

- ERP applications, Enterprise Resource Planning, are focused on planning based on forecasting, procurement management, materials, inventory, accounting information, such as receivables and payments; ERP applications make the leap from the stock based production to requests based production;
- Supplier relationship management (SRM) is the discipline of strategically planning for, and managing, all interactions with third party organizations that supply good and/or services to organization, in order to maximize the value of those interactions. In practice, SRM entails creating closer, more collaborative relationships with key suppliers in order to uncover and realize new value, and reduce risk.
- SCM, Supply Chain Management helps t optimize production process, managing stocks and decreasing the expectation time of customers by fasting up the delivery time; at their full efficiency SCM applications can break the disadvantages generated by logistics;
- Business Intelligence, BI is the picture frame in which are managed the applications described above; it refers to knowledge, skills, technologies, services, risks, security issues, applications and more others that are used for stepping the traditional business into a new era of making business.

Those concepts are relying on the efficiency of the security systems which are incorporated into the functional ones. Security can be very well achieved by implementing a PKI, public key infrastructure, like the one presented in figure 1.

3. SECURITY IN SUPPLY CHAIN

One of the main inhibitors to the uptake of e-business in general, and the adoption of electronic supply chains in particular, has been concern about the security of online transactions. Once organizations can demonstrate to both customers and trading partners the security of their online operations, commercial prospects immediately improve.

It is important to remember that the fundamental goal of electronic supply chain network security is not to prevent the loss of sensitive data, but to maximize the economic return on such data, whilst always maintaining its integrity. Although supply chain security (SCS) is considered an important subject, there has been little formal definition in literature. "The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction or unauthorized contraband, people or weapons of mass destruction into the supply chain"(Doinea, Mihai,2009) the above definition of SCS considers security of supply chains from two aspects, soft and hard. Hard aspect indicates tangible vulnerabilities, such as physical thefts (facilities, equipment, and personnel) or physical damages and terrorism.

Soft aspect refers to intangible vulnerabilities which in the above definition are considered as information theft. The scope of this paper is to clarify information theft and tries to demonstrate details of this phrase connected to information security in e-SC. From an information technology face of security (information security), information theft contains different items such as viruses, worms, Trojan horses, hackers, Trap doors, Logic bombs, port scanning, spoofs, DNS attacks, social engineering, etc.

3.1. Role of Information technology in Supply chain

Information Technology (IT) in SCM enables great opportunities, ranging from direct operational benefits to the creation of strategic advantage. It changes industry structures and even the rules of competition. IT is a key in supporting companies creating strategic advantage by enabling centralized strategic planning with day-to-day centralized operations. In fact supply chain become more market-oriented because of IT usage.
The objectives of IT in SCM are (Simchi et al, 2003):

- Providing information availability and visibility;
- Enabling a single point of contact for data;
- Allowing decisions based on total supply chain information; and
- Enabling collaboration with partners

The functional roles of IT in SCM have been outlined as Follows (Auramo et al,2005). (See figure 2).

ISSN: 1839 - 0846

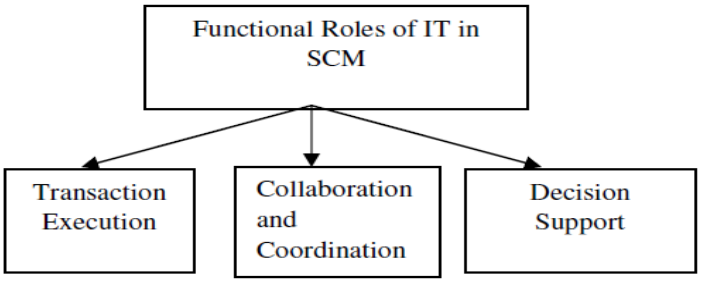

Figure 2; Functional roles of IT in SCM

For the short term, the system must be able to handle day to day transactions and electronic commerce across the supply chain and thus help align supply and demand by sharing information on orders and daily scheduling. From a mid-term perspective, the system must facilitate planning and decision making, supporting the demand and shipment planning and master production scheduling needed to allocate resources efficiently. To add long-term value, the system must enable strategic analysis by providing tools, such as an integrated network model, that synthesize data for use in high-level "what-if" scenario planning to help managers evaluate plants, distribution centers, suppliers, and third-party service alternatives.

3.2. Security in each element of the electoronic supply chain

Every element of the electronic supply chain is affected by issues of trust and security.

- Product development

Open communication is vital during product development, and sharing information and resources within the development team is in everyone's interest. Commercially sensitive information will need to be communicated in a secure online environment, through, for instance, secure e-mail services or virtual private networks.

- Purchasing

This time the goal is transactional confidence. Both parties must be confident in the ability of the other to deliver payment or goods, and to maintain the security of payment details provided - by credit or debit card, for instance. The use of digital signatures supported by certification authorities and encrypted transmissions (such as Secure Socket Layer or other end-to-end security products) can reassure customers that their details will be kept confidential.

- Stock control/inventory

By regulating who has access to your stock control system and who can update records you can make sure that you have an accurate picture of your stock holdings. This is particularly important when online customer/supplier interfaces are in use.

- Order accuracy

Greatly improved by e-mail, fraudulent ordering can be guarded against by the use of digital signatures and Certificate Authorities (CAs). CAs issue and manage security credentials to guarantee people are who they say they are.

- Delivery

Secure delivery information – where the information cannot be intercepted online – means that details of what you have purchased and where it will be delivered are secure. This protects against the possibility of high value items being targeted in transit by thieves.

- Customer service

Increased levels of trust and security in the electronic supply chain lead to better business relationships and greater levels of trading activity.

3.3. Information system Security

Information systems and technologies are a major enabling tool for firms to respond to customers and suppliers in real time resulting in higher sales and higher profits. Information systems have become essential tools for helping enterprises operate in a global economy. The main objectives are reducing inventory levels, improving delivery services, improving the customer service, reducing the cost through the supply chain, and increasing sales. All these will improve the firm's profitability. (Radwan et al,2011 and Ming et al,2009).

The objective of an information system security programmed is to protect an organization’s information by reducing the risk of loss of confidentiality, integrity and availability of that information to an acceptable level. A good information security programmed involves two major elements, risk analysis and risk

ISSN: 1839 - 0846

management. In the risk analysis phase, an inventory of all information systems is taken. For each system, its value to the organization is established and the degree to which the organization is exposed to risk is determined. Risk management, on the other hand, involves selecting the controls and security measures that reduce the organization's exposure to risk to an acceptable level. To be effective, efficient and reflect common sense, risk management must be done within a security framework where information security measures are complemented by computer, administrative, personnel and physical security measures. Here we present Information System (IS) security in terms of the conceptual framework shown diagrammatically in figure 3.(Nachtigal, Sharon, 2009).

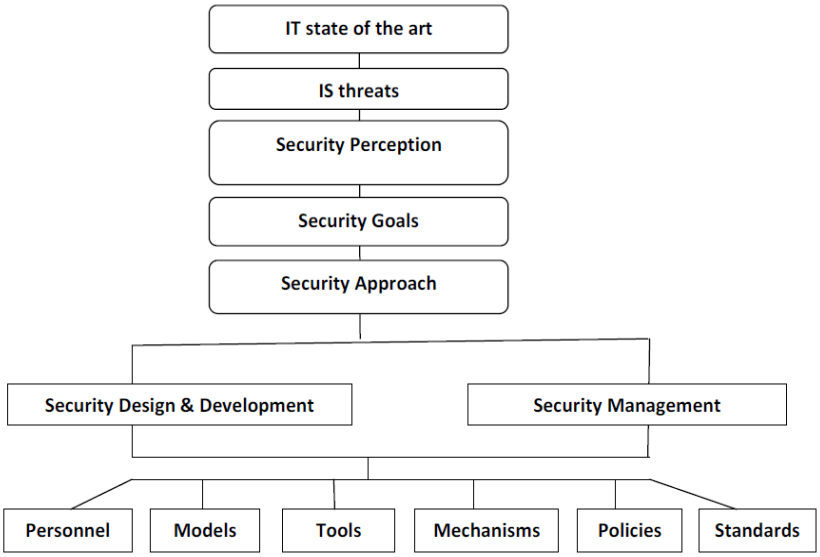

Figure 3; Information System Security framework

The framework above suggests that the approach to security should be derived from the security goals, which are themselves derived from perception of security that is based on identified threats. In this frameworke, security design and development and security management are derived from security approach and in the next section we offer our our information security framework in E-SCM that is based on both security design and development and security management and develop.

4. INFORMATION SECURITY FRAMEWORK IN E-SCM

Information security framework is a comprehensive security framework model that ensures the overall security of information there by eliminating business risks. The comprehensive information security framework should incorporate the following key elements:

- Recommended sound security governance practices (e.g., organization, policies, etc.)
- Recommended sound security controls practices (e.g., people, process, technology)
- A guide to help reconcile the framework to common and different aspects of generally adopted standards
- An analysis of risk or implications for each component of the framework
- A guide of acceptable options or alternatives and criteria, to aid in tailoring to an organizations operating environment
- A guide for implementation and monitoring
- Toolset for organizations to test compliance against the framework

A comprehensive information security framework is the answer for the components to work together, instead of having stand alone components and system. The connected information security framework delivers practical guidance for everyday IT practices and activities, helping users establish and implement reliable, cost-effective IT services. It is obvious that the information security framework for an organization establishes policies and best practices. The framework used for assessing the organization's current information security framework provides a roadmap for the evaluation and improvement of information security policies and practices. The security infrastructure in electronic supply chain (e- scm) needs to have the following basic capabilities;

ISSN: 1839 - 0846

- Identification/authentication:

This is the first step of any security and privacy process: being able to tell who users are.

- Authorization:

Once the system determines who users are and that they are who they say they are it must provide the correct levels of access to different applications and stores of information.

- Asset Protection:

The system must keep information confidential and private. This has become more difficult in the modern e-business environment, where information is traveling across multiple, often entrusted, networks.

- Accountability:

This is the ability to keep track of who has done what with what data. E-business solutions also need to ensure that participants in transactions are accountable.

- Administration:

This involves defining security policies and implementing them consistently across the enterprise infrastructures different platforms and networks.

- Assurance:

This demands mechanisms that show the security solutions are working, through methods such as proactive detection of viruses or intrusions, periodic reports, incident recording, and so forth.

- Availability:

Modern e-businesses must prevent interruptions of service, even during major attacks. This means that the solution must have built-in fault tolerance and applications and procedures to quickly bring systems back online.

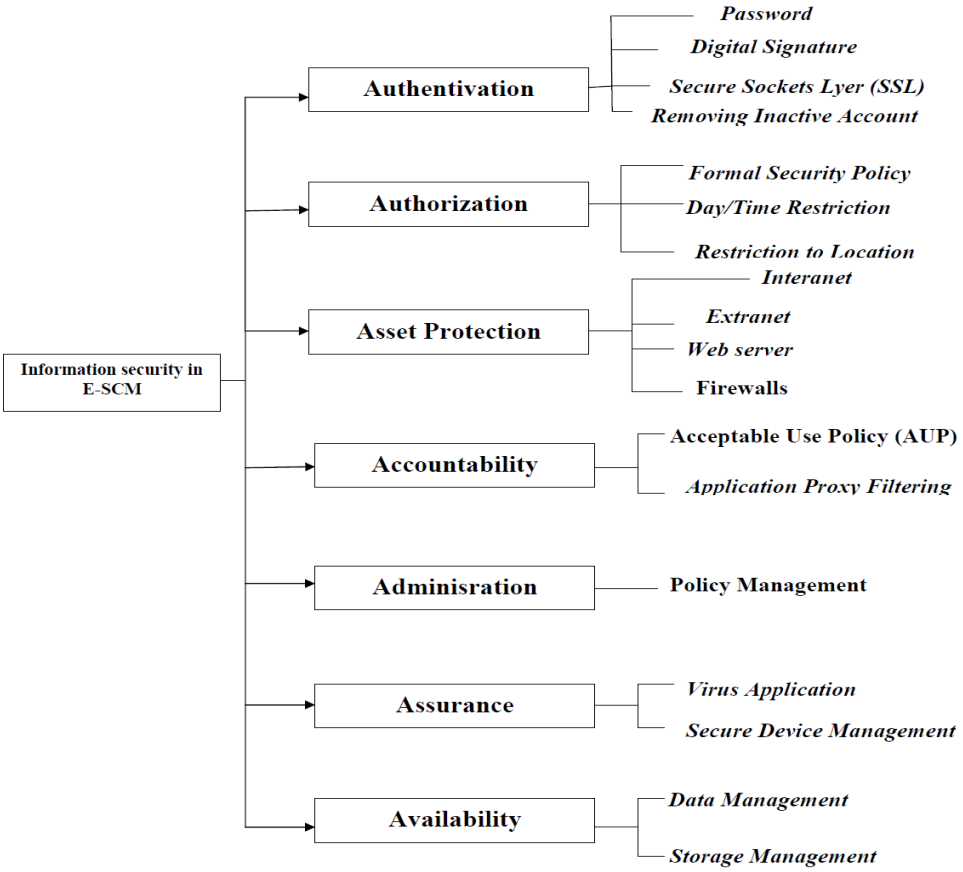

Figure 4; E-Supply Chain Information Security (E-SCIS) framework

Figure 4 describes a framework for identification and application of information security in electronic supply chain. The framework clarifies seven areas that are mentioned and each of them needs several factors to impelement correctly. We just mentioned some of tools and methods which let us make our networks secure facing what mentioned in this frame work under infrastructure for Information Technology area. So it is clear that manager would employ this framework to make sure if security agents in organization have applied security issues in supply chain network.

ISSN: 1839 - 0846

5. CONCLUSION

E-Business systems have become indispensable for most of the large organizations because of the huge development of today's technology and the huge number of competitors that used them. E-Business systems development cause security to be more effective, therefore, as e-business systems will gain new features and the IT&C will be used by more and more users, the security will need to keep the line straight, assuring those information characteristics that always will be necessary. They are dependent on all the application from which they are formed of.

In this era of increased cyber attacks and information security breaches, it is essential that all organizations give information security the focus it requires, specially in supply chain it has vital role which can not be overlooked by the organization that are involved. To ensure information security, the organization should understand that information security is not solely a technological issue. The organization should also consider the non-technical aspect of information security while developing the information security framework. This paper examined information security and e-SC concepts.

The focus of this paper was information security in electronic suplly chain management while use e-business in its transaction. Through the paper, one realizes that IS in every information based-system will be vital and need to be developed in electronic supply chains because in some cases the importance of Information System is low and in others high. Our propused framework highlights major fileds in supply chain information security which managers can reap the benefits of studying these factors.

REFERENCES

1. Manivannan Senthil Velmurugan,(2009)," security and trust in e-business: problems and Prospects",*International Journal of Electronic Business Management*, 7(3) 151-158.
2. Luo yixin, (2011)." Study on the Current Situation of Information Security and Countermeasures in China" Energy Procedia 5 392–396
3. Yeung JHY, Selen W, Zhang M, Huo B,(2009)." The effects of trust and coercive power on supplier integration", *International Journal of Production Economics*; 120:66.
4. Ipek Koçoglua, Salih Zeki Imamo glua, Hüseyin Incea, Halit Keskin, (2011). "The effect of supply chain integration on information sharing: Enhancing the supply chain performance," Procedia Social and Behavioral Sciences 24, 1630–1649.
5. Simchi-levi, David , Philip Kaminsky and Edith Simchi-levi (2003), "Managing The Supply Chain: The Definitive Guide For The Business Professional", (Hardcover - 12-2003)
6. Li S, Lin B.(2006). "Accessing information sharing and information quality in supply chain management."Journal of Decision Support Systems; 42:1641-1656.
7. Gaile-Sarkane, E. (2005) "Basics of E-Marketing." Publishing House of RTU. 232 pp.
8. Poirier, C., Bauer, M. (2000), "E-supply Chain: Using the Internet to revolutionize your business", Berrett-Keohler Publishers, San Francisco, CA.
9. Williams, L.R., Esper, T.L., & Ozment, J. (2002), "The electronic supply chain: Its impact on the current and future structure of strategic alliances, partnerships and logistics leadership", *International Journal of Physical Distribution & Logistics Management*, 32(8), 703-719.
10. Closs, D.J. and McGarrell, E.F. (2004) "Enhancing security throughout the supply chain," Special Report Series, IBM Center for the Business of Government.
11. Asanka Hiroshana Horadugoda Gamage,(2007), "E-Business Impact on SCM in the apparel industry operating between a developing and a developed economy," A Thesis submitted for the degree of Doctor of Philosophy, Brunel University.
12. Flynn BB, Huo B, Zhao X. (2010), "The impact of supply chain integration on performance: A contingency and configuration approach". *Journal of Operations Management*; 28: 58-71.
13. Doinea, Mihai,(2009)," E-Business Security Architectures" Informatica Economică, 13(9).
14. Auramo, Jaana,; Jouni Kauremaa and Kari Tanskanen,(2005),"Benefits of IT in Supply Chain Management: An explorative study of progressive companies" International Journal of Physical Distribution and Logistics Management; 35,2; Academic Research Library pg. 82.
15. Radwan, A., and Majid Aarabi,(2011)," Modeling Supply Chain Management Information System Using ARIS Framework" Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management Kuala Lumpur, Malaysia, January 22 – 24.
16. Ming-Chang Lee, Mei-Wen Han,(2009), "E-Business Model Design and Implementation in Supply Chain Integration,", International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 001-004.
17. Nachtigal, Sharon, (2009)" E-business Information Systems Security Design Paradigm and Model" Thesis submitted to The University of London for the degree of Doctor of Philosophy.