12-1-2009

Electronic-Supply Chain Information Security: A Framework for Information

Alizera Bolhari
Shahid Beheshti University

DOI: 10.4225/75/57b404e730ded
7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

Electronic-Supply Chain Information Security: A Framework for Information Security in e-SCM (e-SCIS)

Alizera Bolhari
Shahid Beheshti University, Tehran, Iran

Abstract

Over the last few years, the materials and distribution management has developed into a broader strategic approach known as electronic supply chain management by means of information technology. This paper attempts to visibly describe supply chain management information security concepts which are necessary for managers to know about. So, the depth of information presented in this paper is calibrated for managers, not technical security employees or agents. Global supply chains are exposed to diverse types of risks that rise along with increasing globalization. Electronic supply chains will be more vulnerable from information security (IS) 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.

Keywords

Electronic-supply chain management, information technology, information security, vulnerability

INTRODUCTION

Internet users have to prove their identity when accessing services or personal information from web services (service providers). This authentication is generally achieved through the use of identifiers and passwords. With the emergence of the Internet and its substantial popularity, users have to manage a growing numbers of login/passwords which represent their identity across different Service Providers (SPs). The management of these is often difficult as the user does not remember every identifier associated with each web service. In addition, the use of passwords raises a problem of security, with for example having an identity compromised, theft or misused (Schneier, 2004). Indeed, password authentication relies upon the use of a secret knowledge shared between two parties that could be easily disclosed either by the user's behaviour or by a bad implementation of the authentication protocol at the Service Provider. In the first case, the user is responsible to protect, manage and update his passwords on a regular basis and to utilize a different one for each service (Warren, 2006). However, this is not the case for all users who often write them down on paper or a post-it, or just use the same password for every service. As such, Service Providers also have to be careful about the implementation of such an authentication technique and the reliability it is assumed to have. In addition, other threats such as eavesdropping could also reveal the secret information if the channel between end-user devices is not secured (Warren, 2006). Currently, the most frequent form to secure the exchange of credentials is to use the Secure Socket Layer (SSL) protocol with a server side certificate, but this is not always utilised. Taking this into account, the research has proposed a novel approach where a smartcard will be utilised to provide transparent authentication of the user from his device. This approach removes any inconvenience for the user in having to remember username and password information for each service and provides the opportunity to improve the level of security through using asymmetric cryptography.

This paper is organized in five sections, beginning with an overview of smart cards technologies. The paper will then proceed to discuss current research in to the area of federated identity, specifically focussing upon the work of Shibboleth and Liberty Alliance. The third section provides a detailed description of the novel approach; and the penultimate section discusses the overall concept, with a discussion on the advantages and disadvantages. Finally, the conclusions are presented in section four.

SUPPLY CHAIN

Stages or steps which are built to fulfill the demand of the customers are called Supply chain (SC). Classic SCs usually includes suppliers, manufacturers, wholesalers, retailers, and end customers (Luong and Phien, 2007). Christopher (1992) states that an appropriate definition of SC is ''a network of organizations that are involved, through upstream and downstream linkages, in different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer'' from a logistical point of view. Ayers (2001) defines SC as "life cycle processes comprising physical, information, financial and knowledge flows whose purpose is to satisfy end-user requirements with products and services from multiple linked suppliers".

Supply chain management (SCM), offers a way to improve the competitiveness of the industrial environment, and involves planning and managing different flows through multi-echelon of design, production, shipment and distribution (Christopher, 1992; Sha & Che, 2005, 2006). Ayers (2001) defines SCM as "design, maintenance and operation of supply chain processes for satisfaction of end-user needs". Figure 1 shows simple and extended structure of a sample supply chain.

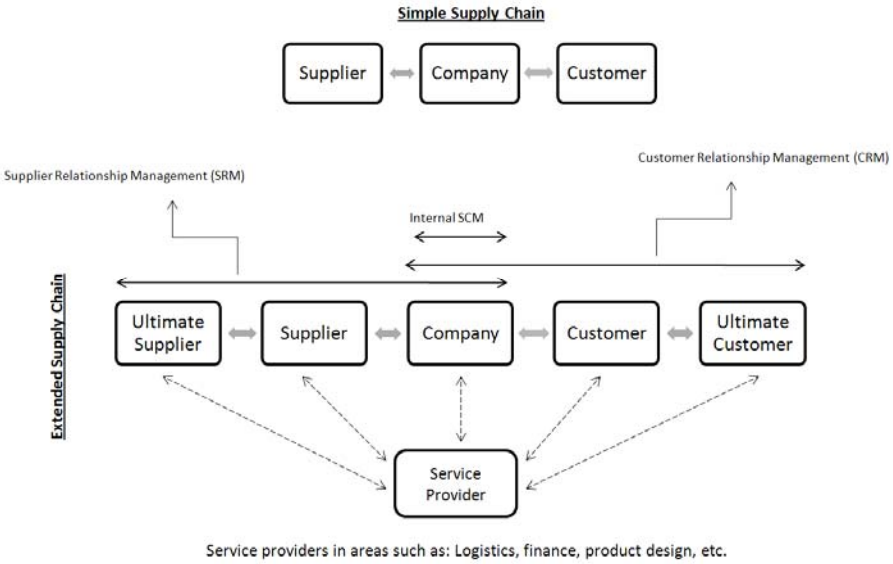

Figure 1- Simple and Extended SC Structure (Adapted from Hugos, 2006)

The network view of the SC (Figure 2) encompasses more exchanges of both information and material flows in either reciprocal way. The central company (dark grey) at the centre is in contact with many suppliers and customers across the world through either electronic or non-electronic methods.

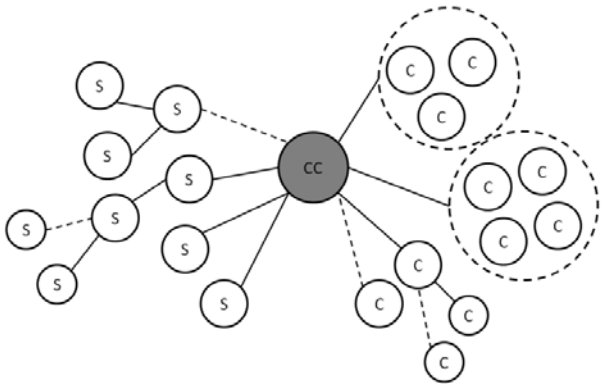

Figure 2 - Network view of supplier–customer interactions (Adapted from Kemppainen and Vepsalainen, 2003)

Three flows are defined in the supply chain: materials, information and financial (cash) flows which are presented in figure 3.

- Material flows. All tangible products, new materials and supplies that flow along the chain. Returned and disposed products are also included in the material flows.
- Information flows. Information flows consist of all data related to demand, schedules shipment, orders, and returns. The focus of this paper is on information flow in supply chain management.
- Financial flows. All credit-card information and authorization, payments, transfers of money, e-payments and credit data, payment schedules, is called financial flows.

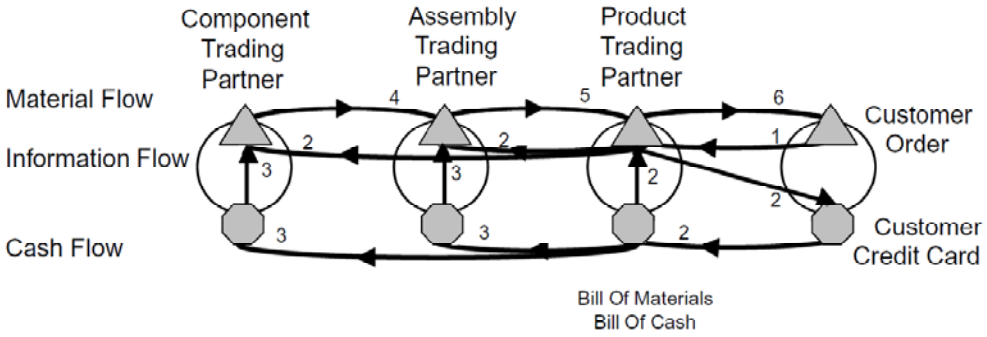

Figure 3 - Sample diagram of flows in SC from customer order to product delivery (Walker, 2005)

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 and Bauer, 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, Esper, & Ozment, 2002).

Poirier and Bauer (2000) draw attention to three elements in the preparation and execution of e-SCM: e-network (fully connected end-to-end business networks)**,** responses (customer responses form the central theme of the supply chain strategy) and technology (each of the above constituents can achieve the goal of the supply chain by being supported with technology). These three constituents could be seen as the "input" into e-SCM working together to reach the aim (output) of the supply chain (customer satisfaction).

BASIC CONCEPTS OF SECURITY, THE SECURITY TRINITY

The three legs of the "security trinity" (figure 4) are the basis for network security. The security trinity is the base for all security policies that an organization develops (Canavan, 2001).

Figure 4 - The security trinity

Prevention

In order to provide some level of security, implementing measures to prevent the use of vulnerabilities is necessary. In developing network security schemes, one should emphasize preventative measures over two other legs: It is easier, more resourceful, and much more economical to prevent a security breach than to detect or respond to one.

Detection

Once preventative measures are applied, procedures need to be established to detect potential vulnerabilities or security breaches; in the event preventative measures not succeed. The sooner a problem is detected the easier it is to correct and cleanup.

Response

Organizations should develop a map that identifies the suitable response to a security breach. The map should be in writing and should identify who is responsible for what actions and the different responses.

Network security is not a technical problem; it is a business and people problem. Developing a security plan/map that fits the organization's business process and getting people to comply with the plan/map is the difficult part. Companies need to answer several fundamental questions, including the following:

- How does your organization define network security?
- How does your organization determine what is a suitable level of security?

In order to answer these questions, it is necessary to decide what you are trying to protect.

KEY PRINCIPLES OF NETWORK SECURITY

Network security orbits around the three key principles of confidentiality, integrity, and availability (C-I-A). Depending on the application, one of these principles might be more important. To make CIA concept clear examine an agency which encrypts an electronically transmitted document to prevent an illegal person from reading the contents. So, *confidentiality* of the information is vital. If someone succeeds in breaking the encryption cipher and then, transmits a modified encrypted version, the *integrity* of the message is under question. On the other side, an organization such as eBay.com would be severely spoiled if its network were out of commission for a period of time. Thus, *availability* is a key concern of such e-commerce organizations (Cole, et al., 2005).

Canavan (2001) mentions that information security is not just about protecting properties from outsiders, but ensuring sufficient physical security such as hiring right personnel, developing and holding procedures and policies, strengthening and monitoring networks and systems, etc. are all key elements.

E-SUPPLY CHAIN SECURITY

A survey conducted jointly by the American Society for Industrial Security and Pricewaterhouse-Coopers (ASIS/PWC) in 1999, reported that Fortune 1000 companies lost more than forty five billion dollars from theft of "proprietary information." The survey reported the following:

- 45 percent said that they had experienced a financial loss as because of information loss, theft, or misappropriation.
- The responding companies reported, in average, 2.45 incidents with an approximate cost of $500,000 for each incident.
- The number of reported incidents had risen over the last seventeen months.

Although SCS is considered an important subject, but there have been few formal definitions in literature. One appropriate definition which is suitable for this research is presented by Closs and McGarrell (2004, p.8): “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”.

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 is 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. Table 1 illustrates a concise description of some threats, vulnerabilities and attacks which are called factors of decreasing security level.

Table 1- Description of some threats, vulnerabilities and attacks (overlaps may exist for coverage purposes)

Item	Description	Reference
Virus	A program that can be broken up into three functional parts; Replication, Concealment, Bomb (Precise definition has been debated for many years)	Brenton, C., Hunt, C., (2001)
Worm	A self-supporting program which will only maintain a functional copy of itself in active memory; it will not even write itself to disk	Brenton, C., Hunt, C., (2001)
Trojan horse (Trojans)	Malicious software that pretends to be a benign application. Trojans are seemingly harmless that hide a malicious activity, such as a keystroke. The visible application may or may not do anything that is actually	Bhaiji, Y., (2008), Brenton, C., Hunt, C., (2001)

	useful. The hidden application is what makes the program a Trojan horse.	
Flooding	When an excessive amount of unwanted data is sent, resulting in disruption of data availability.	Bhaiji, Yusuf, (2008)
Hacker	Someone with a deep understanding of computers and/or networking. Hackers are not satisfied with simply executing a program; they need to understand all the nuances of how it works. A hacker is someone who feels the need to go beyond the obvious. Hacking can be either positive or negative, depending on the personalities and motivations involved.	Brenton, C., Hunt, C., (2001)
Trap door (Back door)	A trap door or back door is an undocumented way of gaining access to a system that is built into the system by its designer(s). It can also be a program that has been altered to allow someone to gain privileged access to a system or process.	Canavan, John E. (2001)
Logic bomb	A program or subsection of a program designed with malevolent intent. It is referred to as a logic bomb, because the program is triggered when certain logical conditions are met. This type of attack is almost always perpetrated by an insider with privileged access to the network. The perpetrator could be a programmer or a vendor that supplies software.	Canavan, John E. (2001)
Port scanning	A method used to enumerate what services are running on a system. Intruder sends random requests on different ports, and if the host responds, intruder confirms that the port is alive.	Bhaiji, Yusuf, (2008)
Spoof	Covers a broad category of threats. Spoof entails falsifying one's identity or masquerading as some other individual or entity to gain access to a system or network or to gain information for some other unauthorized purpose. Some kinds of spoofs: IP Address Spoof, Sequence Number Spoof, and Session High-jacking	Canavan, John E. (2001)
DNS attack	Domain Name Service attack refers to manipulation of the domain name registry to redirect a URL. Some major spoofs of DNS are Man in the Middle Attack (MIM), DNS Poisoning, and Redirect.	Canavan, John E. (2001)
Social engineering (Hoax)	Meet all the criteria of a normal virus, except they rely on people to spread the infection, not a computer	Brenton, C., Hunt, C., (2001)
Dumpster diving	The process of gathering information by going through garbage. Computer printout is of particular value in dumpster diving. Hackers look for information such as system account names, source code, or customer account numbers.	Canavan, John E. (2001)
Sniffing	A software that uses a network adapter card in promiscuous mode to passively capture all network packets	Bhaiji, Yusuf, (2008)
Website defacement	Posting some message on websites protesting something or other. Web site defacements are usually achieved by exploiting some incorrect configuration or known vulnerability of the Web server software, or by exploiting some other protocol-based vulnerability of the server's operating system.	Canavan, John E. (2001)
War dialing	Brute-force method of finding a back door into an organization's network. It is particularly effective against a perimeter defense. The program logs a telephone number whenever it finds a modem. Later after the program has called every extension, the hacker can review the log for modems and go back and attempt to break into the system to which the modem is connected to gain access to the	Canavan, John E. (2001)

	network.	
DoS/DDoS Attack	Denial of Service deprives legitimate users from access to services or resources. Distributed DoS attacks amplify DoS attacks in that a large number of compromised systems coordinate collectively to flood the victim, causing DoS for users of the targeted systems. DoS attacks do not require a great deal of experience, skill, or intelligence to succeed. DoS/DDoS Attack include Ping of death, SYN flooding (synchronize sequence number), SPAM, viruses, worms and Smurf attack.	Bhaiji, Yusuf, (2008), Canavan, John E. (2001)
Password Cracking (Directory-based attack)	Programs that decipher password files. They are able to decipher password files by utilizing the same algorithm used to create the encrypted password. Some methods are brute force attacks, Trojan horse programs, IP spoofing, and packet sniffers.	Canavan, John E. (2001), Bhaiji, Yusuf, (2008)

On the other hand, there are some methods or tools which let us make our networks secure facing what mentioned in table 1. These methods or tools are shown in table 2 which are called factors of increasing security level.

Table 2- Description of some securing methods or tools (overlaps may exist for coverage purposes)

Item	Description	Reference
Password	The first and usually only means of identification and authentication. Even though passwords are the most widely deployed scheme of authentication, they are perhaps the weakest link in any system security scheme.	Canavan, John E. (2001)
Firewall	Fundamental component of any perimeter defense. A firewall is usually not a single system; it is actually a collection of components. A firewall is usually placed between two networks to act as a gateway. A personal firewall can be much more effective than a perimeter firewall in protecting the user's workstation.	Canavan, John E. (2001), Cole, E., Krutz, R., and Conley J. W. (2005)
Virtual Private Network (VPN)	A means of transporting traffic in a secure manner over an unsecured network. A VPN usually achieves this by employing some combination of encryption, authentication, and tunneling.	Canavan, John E. (2001)
Digital Signature	Allows a receiver to authenticate (to a limited extent) the identity of the sender and to verify the integrity of the message. Digital signatures are used to ensure message integrity and authentication.	Canavan, John E. (2001)
Secure Sockets Layer (SSL)	Providing security when transmitting information on the Internet. When used with a browser client, SSL establishes a secure connection between the client browser and the server. SSL works between the application and transport layers of the network protocol stack to ensure security of applications on the transport layer.	Canavan, John E. (2001), Cole, E., Krutz, R., and Conley J. W. (2005)
Virus Applications	Protection against viruses can be provided by antivirus applications that provide frequent upgrades for virus signatures.	Cole, E., Krutz, R., and Conley J. W. (2005)
Available Disk Space	Limiting the amount of disk space allocated to each end user. Giving users unlimited disk space may end up requiring the purchase of additional disk capacity and may result security issues, e.g. server crash.	Canavan, John E. (2001)
Formal Security Policy	Set of rules and procedures that regulate how an organization manages, uses, authorizes, protects, and distributes all information that directly or indirectly pertains to that organization. Some such policies are E-mail Policy, Disclosure of Passwords (Passwords	Canavan, John E. (2001), Cole, E., Krutz, R., and Conley J. W. (2005)

	Secrecy), Liability Policy, Information Integrity and Confidentiality Policy, New Account Policy.	
Time/Day Restrictions	Restricting end user access to business hours only, especially for those employees who are authorized to access and use sensitive and/or confidential data.	Canavan, John E. (2001)
Restrictions to Location or Workstation	Restricting end users who are authorized to enter sensitive transactions or who perform particularly sensitive and/or confidential work. Access to the server itself should be restricted.	Canavan, John E. (2001)
Removing Inactive Accounts	Deleting any accounts that are no longer required on a regular base. Accounts for users or employees no longer with the organization should be deleted. Hackers frequently try to exploit inactive accounts for the initial break into a system or as a means to gain access to a network.	Canavan, John E. (2001)
Segmenting LAN Traffic	With the Ethernet protocol, any device on a network segment can monitor communications between any other devices on that same network segment. Whenever possible, organizations should segment their networks for both security and performance purposes. Segmenting networks prevents packets from traversing the entire network.	Canavan, John E. (2001)
Encryption, Digital Signatures, and Certification Authorities	For the exchange of information and commerce to be secure on any network, a system or process must be put in place that satisfies requirements for confidentiality, access control, authentication, integrity, and non-repudiation.	Canavan, John E. (2001), p. 38

FRAMEWORK OF IT IN SCM

Figure 5 describes a framework for identification and application of information technology in SCM. (Gunasekaran and Ngai, 2004). The framework clarifies six areas and their role in SCM. Here we examine this framework as the information security point of view. First a quick review on the framework and then the novel information security in e-SC framework is presented (see figure 6).

Strategic planning for IT: Making and managing long-term decisions (e.g. selection and implementation of IT) with the purpose of achieving an effective supply chain is discussed in strategic planning for IT.
Virtual Organization/Virtual Enterprise (VO/VE): In today's business environment, one of the most important strategic applications of IT is developing a VO/VE. Virtual organization becomes a vital strategy for having an agile supply chain. This type of organization is made up of partners who are collaboratively offering various products/services.

E-commerce: It helps inter-organizational communication and decreases cycle-times and develops collaborative environment. E-commerce provides chances of expanding markets worldwide. This requires a SCM system, which effectively satisfy the increasing demand.
Infrastructure for IT: High-speed Internet services for processing voluminous data and high-speed internet portals are examples of infrastructures for IT.

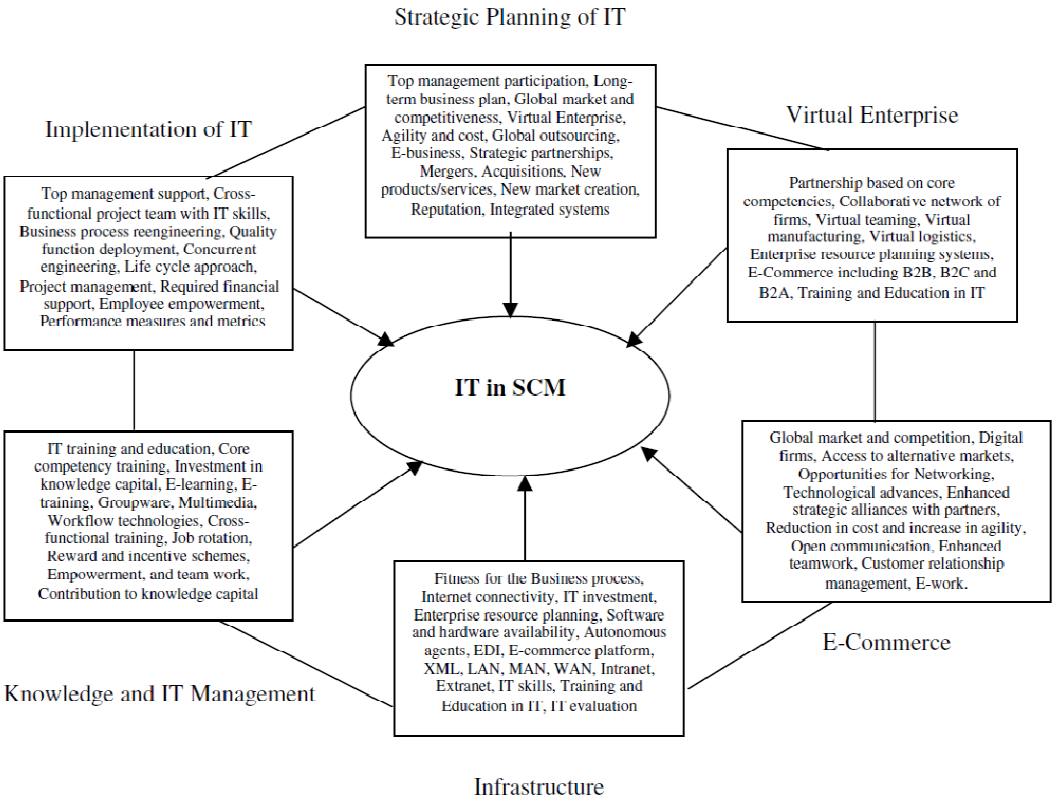

Figure 5 - Framework of IT in SCM (Gunasekaran and Ngai, 2004)

Knowledge and IT management: One of the strategic uses of IT in today's business environments is knowledge management. A lot of organizations build KM system for organizational learning. This needs a systematic evaluation of various knowledge and IT management strategies and methods.

Implementation of IT: Implementation of IT to reach agility in a supply chain needs a strong team that can include knowledgeable IT managers from different functional areas. Top management support and involvement and a well documented implementation plan are required for IT in developing an effective supply chain.

PROPOSED FRAMEWORK OF E-SUPPLY CHAIN INFORMATION SECURITY

The proposed framework's addresser is organization's managers whose job is not engaged with technical security concepts. They know the overall concepts of security, but not in-action work. e-Supply Chain Information Security (e-SCIS) framework (figure 6) describes IT items in each six area which needs to be checked with IS factors (Tables 1 and 2) if applied in e-supply chain network, considering the needed level of security. For example, in the area of infrastructure, security issues for internet connectivity should be examined due to what mentioned in tables 1 and 2. So managers would employ this framework to make sure if security agents in organization have applied security issues in supply chain network.

Factors of Decreasing Security Level (Table 1)

Area	IS factors to be considered in each item below
Strategic planning for IT	Virtual Enterprise, Agility and cost, Global outsourcing, E-business, Strategic partnerships, Mergers, Acquisitions, New products/services, New market creation, Reputation, Integrated systems
Virtual enterprise	Collaborative network of firms, Virtual teaming, Virtual manufacturing, Virtual logistics, Enterprise resource planning systems, E-Commerce including B2B, B2C and B2A
E-commerce	Global market and competition, Digital firms, Access to alternative markets, Opportunities for Networking, Technological advances, Enhanced strategic alliances with partners, Reduction in cost and increase in agility, Open communication, Enhanced teamwork, Customer relationship management, E-work
Infrastructure for IT	Internet connectivity, Enterprise resource planning, Autonomous agents, EDI, E-commerce platform, XML, LAN, MAN, WAN, Intranet, Extranet, IT skills, Training and Education in IT, IT evaluation
Knowledge and IT management	E-learning, E-training, Groupware, Multimedia, Workflow technologies, Cross-functional training, Empowerment and team work, Contribution to knowledge capital
Implementation of IT	Cross-functional project team with IT skills, Project management, Required financial support, Employee empowerment, Performance measures and metrics

Factors of Increasing Security Level (Table 2)

Figure 6 - e-Supply Chain Information Security (e-SCIS) Framework

FUTURE WORK

As mentioned earlier, there are limited researches in literature concerning e-supply chain information security. So there are still areas in this field which need researchers' attention for future work, e.g. potential risks and risk management in e-supply chains. The proposed information security framework can be a good starting point for future studies. Each six area of e-SCIS framework (strategic planning for IT, virtual enterprise, e-commerce, infrastructure for IT, knowledge and IT management and Implementation of IT) can be a part of future work. For example one can focus on virtual enterprise and investigate information security issues concerning IS factors.

CONCLUSION

This paper deeply examined information security and e-SC concepts. Since there are just a few papers about information security in literature, this issue needs further empirical researches. The focus of this paper was information security in supply chain management. Through the paper, one realizes that IS in every information based-system will be vital. In some cases the importance of IS is low and in others high. It is obvious that IT has had great influence on achieving an effective SC and going toward e-SCM. Managers will benefit from the results of examining proposed framework (e-SCIS) shown in figure 6. Throughout the study of this framework, major fields in supply chain information security are highlighted and managers can easily study information security factors (tables 1 and 2) as a checklist.

For further research on this subject, it is recommended to researchers to examine this e-SCIS framework and conduct more empirical research.

REFERENCES

Ayers, James, B. (2001), *Handbook of Supply Chain Management*, St. Lucie Press, Boca Raton, 4-5

Bhaiji, Yusuf, (2008), *Network Security Technologies and Solutions* (CCIE Professional Development Series), Cisco Press; 1 edition

Brenton, Chris, Hunt, Cameron, (2001), *Active Defense — A Comprehensive Guide to Network Security*, SYBEX Inc., CA

Closs, D.J. and McGarrell, E.F. (2004), *Enhancing security throughout the supply chain*, Special Report Series, IBM Center for The Business of Government

Canavan, John E. (2001), *Fundamentals of Network Security*, Artech House Publishers; 1st edition

Christopher, M. G. (1992), *Logistics and supply chain management: strategies for reducing costs and improving services*, London: Pitman.

Cole, E., Krutz, R., and Conley J. W. (2005), *Network Security Bible*, Wiley Publishing, Inc. Indianapolis, Indiana

Gunasekaran, A., Ngai, E.W.T. (2004), *Information systems in supply chain integration and management*, European Journal of Operational Research 159, 269–295

Hugos, M. (2006), *Essentials of Supply Chain Management*, John Wiley & Sons, Inc., Hoboken, New Jersey

Kemppainen, K., Vepsalainen, A.P.J., (2003), *Trends in industrial supply chains and networks*, International Journal of Physical Distribution and Logistics Management 33 (8), 701– 719

Luong, Huynh Trung, and Phien, Nguyen Huu, (2007), *Measure of bullwhip effect in supply chains: The case of high order autoregressive demand process*, European Journal of Operational Research, Volume 183, Issue 1, Pages 197-209

Poirier, C., Bauer, M. (2000), *E-supply Chain: Using the Internet to revolutionize your business*, Berrett-Keohler Publishers, San Francisco, CA

Sha, D. Y., & Che, Z. H. (2005), *Virtual integration with a multi-criteria partner selection model for the multi-echelon manufacturing system*, International Journal of Advanced Manufacturing Technology, 25(7–8), 739–802

Sha, D. Y., & Che, Z. H. (2006), *Supply chain network design: partner selection and production/distribution planning using a systematic model*, Journal of the Operational Research Society, 57(1), 52–62

Thibault, M., Brooks, M.R. and Button, K.J. (2006), *The response of the US maritime industry to the new container security initiatives*, Transportation Journal, Vol. 45 No. 1, pp. 5-15

Walker, W. T., (2005), *Supply chain architecture: a blueprint for networking the flow of material, information, and cash*, CRC Press LLC, Florida

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

Williams, Z. and Lueg J. E. and LeMay S. A. (2008), *Supply chain security: an overview and research agenda,* The International Journal of Logistics Management, Vol. 19 No. 2, pp. 254-281

COPYRIGHT