Information Security Issues in the Management of the Supply Chain

by

Anand S. Kunnathur
Sandra Pavuk

College of Business, University of Toledo
Email: **akunnat@utnet.utoledo.edu**

Information Security Issues in the Management of the Supply Chain

Abstract

Strategic, logistical, and other operational issues in managing the supply chain have received a lot of attention from researchers. However, little attention appears to have been paid to ensuring the security of information flows in the supply chain. Security of the information flows is not only a necessity for ensuring smooth operation of the supply chain, but also for preserving relationships and for maintaining a competitive strategic posture. The weakest link, as the cliché goes, defines the chain. In trans-border, multinational environments, there are many links in the chain and not all of the same level of security. This research will frame the research questions, after surveying relevant literature, and develop in some additional detail the issues related to managing the supply chain in a global trans-border data flow environment.

Introduction

The supply chain covers all those activities associated with flow and transformation of goods from the raw materials to the end user. It includes sourcing and procurement, production scheduling, order processing, cash flow, inventory management, transportation, warehousing, and customer service.

One important element of the supply chain is the information system, which monitors these activities and supports communication among them. It is the working of this communication system that exploits opportunities for competitive advantage in the supply chain. Today, the changes in information systems are not linear. The Internet is transforming the way business is done. The new economy is all about E-commerce.

In business-to-consumer transactions, E-commerce makes buying more efficient by reducing or eliminating costs throughout the system. Lead times are also seeing reductions, which helps businesses respond to their customers faster. In business-to-business transactions the impact of e-commerce is enormous. Product development times are significantly shorter and the information flows between companies are more streamlined than ever before. Business buyers can be assured that their purchases provide their companies the highest possible value.

For this reason supply chains have also seen significant development in recent years with the rise of the Internet. But opportunities bring challenges. The traditional supply chain management practices are being challenged and transformed as per the need to remain competitive in the market. Some of the challenges for competition in the e-business environment are the synchronization of the supply chains, pace of execution, global information and material movement issues, organizational systems, measurement systems, legal issues, security issues, and the development of vendor channels.

The global supply chain has many different challenges that come with the trans-border transportation of goods and services. Many products are no longer local to the production area and different product parts are likely coming from different countries. This requires a lot of communication and information sharing between countries. Longer and more complex supply chains are being created as companies try to find the best products, parts and prices all over the globe. Global supply chains require a different focus. The computer systems in global supply chains need to be more effective, farther reaching, and compatible. Through these computer systems a continuous pipeline of

information should be maintained to ensure the supply chain is communicating effectively and efficiently. Global supply chains require that their logistics processes and information flows be streamlined.

The need for timely and correct information to grease the wheels of E-commerce is an imperative, which more and more organizations are coming to grips with. Through the 1990s, there was a trend away from building an information-handling infrastructure in organizations. In one sense, it was a calculated decision to relinquish absolute control over the information assets of the organization in favor of third party processing and handling, and outright outsourcing. The acquisition of logistical support that information processing capabilities provide in maintaining the smooth operation of a global supply chain are in a way a revisitation of the downsizing decisions made in the 1990s. Whichever way this plays out, the reality of having to regain control of information assets is an imperative organizations can ill afford to ignore, given the need for securing information flows in the global supply chain.

Information security is at risk when unauthorized usage occurs in an organization's e-commerce interface. The abuse of the interface for unauthorized access to sensitive organizational information is a primary security concern. To protect organizational information one must try to avoid security disruptions, protect from any interference with the information flows, and develop trust among all supply chain members. This is more critical in a global E-commerce environment with multiple organizations, intermediaries, and nations involved. The stakes are high in having to maintain smooth flow of goods and services. Massive and costly disruptions can occur if

information processing and information flows are compromised, especially due to security breaches.

Literature Survey

The literature surveyed in this paper highlights many relevant issues pertaining to securing information flows in the supply chain. Some of the ideas and issues obtained from the literature are outlined below.

Coffee (2004) has indicated that securing information flows has become more difficult because of the emergence of web-based communications, the Internet, wireless networks, etc. Those conclusions are also supported by an Entrust white paper, published in 2004, which adds that with the openness of e-business comes the reality of information exposure and risk. With some organizations creating extranets for vendors, suppliers, and preferred customers to tie their networks together, companies are realizing the importance of information security (Entrust, 2004). Other security considerations discussed in the literature include the general openness of the web environment, remote access, and mobile data devices (Pironti, Unisys)

Hale et al (2004), have defined the relationship between information and data security breaches, which are also applicable to the supply chain. They identify examples of the different types of information security breaches, such as: interception/theft, interruptions/destruction, modification, or fabrication. By interception of data is meant the accessing of an information asset in an unauthorized manner, such as acts of espionage through the Internet or wireless networks by competitors. Interruptions or destructions are described as bringing down an IT infrastructure with a virus or other

mode of attack to web server or storage system. Modification is, as in, tampering with an information asset, for example, in a wireless network or website. Competitors could be trying to profit from or cause damage through misinformation. Fabrication is defined as the counterfeiting of an information asset, potentially used in hijacking a website to gain access to information. All of the information security breaches are considered cyber-attacks that are a vulnerability for any organization. With the expansion of global supply chains and the usage of the Internet, the probability for these types of attacks to occur can only increase**.** Possible solutions to these information security breaches include encryption, firewalls, employee education, and back-up procedures (Hale et al, 2004).

"However, the Net was not originally designed for security. Rather, its open architecture was intended to enable and encourage the free flow of information between users, not to restrict it, resulting in information vulnerabilities."(Hale et al, 2004)
Hale et al, (2004) further observe that as the US economy has become more service-oriented, firms have found that by developing and strategically using information they are better able to satisfy customers and maintain a competitive advantage. As a consequence, many key information assets are in electronic form to make their modification and transmission faster and easier.

"Information security is now a critical component of long-term company performance and should be directed strategically by top management" (Hale et al, 2004). They go on to discuss how organizations should respond to information security threats. They observe that organizations must value their information assets, assess threats, and then evaluate the costs of securing those assets. "When companies are forced to take a

reactive, ad hoc approach to information security rather than a proactive, strategic one, information remains vulnerable. Even more alarming is that critical information may be attacked, accessed, copied, altered, or stolen without a company's knowledge."(Hale et al, 2004) It can be very dangerous for a company to only rely on a reactive strategy when dealing with information security issues, especially when the company may not even know what type of information breach has occurred. The implications for this in the context of the global supply chain are that it might be difficult for a company to determine where and when the information breach occurred if they don't have a comprehensive information security system in place.

Wagner (2003) considers that web security standards will face a long road to maturity as web services become more complex and involve interactions between multiple parties. Users will begin to require more versatile security. "Unfortunately, the progress towards establishing a set of web security standards that work together is being slowed by political battles between suppliers."(Wagner, 2003)

From the perspective of general strategy formulation, the supply chain must deal with disruptions of all types and there is a strong need for a business continuity plan with contingency planning, especially to maintain the efficiency of the supply chains. (Reddy, 2004) This idea leads directly into the main topic of information flows. Information flow is critical to the efficiency of the entire supply chain. "Such information visibility requires at least two things: (1) event-driven data on supply chain operations, including security chain-of-custody information and (2) a tight integration of information systems across suppliers, manufacturers, logistics providers, and customers."(Lee, et al, 2003)

An Entrust (2004) white paper argues that, in order to secure data that is dispersed across a diverse environment, a solution needs to be scalable, yet comprehensive enough to deliver authentication, access control, encryption and digital signatures- that enable accountability and privacy.

Murtaza et al (2004) look at the major information security concerns of an online, e-marketplace supply chain that include: confidentiality, industry-wide standards, and integration of the company's system with the e-marketplace.

A few of the authors introduced information security issues raised with the new RFID technology. For example, “Information can be written to the devices at any point in the supply chain and the chips can transmit data to servers automatically”, asserts Barry (2005). The RFID technology is also vulnerable when it is stored on the chip itself and also when it is written to, or read from the chip (Willoughby, 2004). A related information security topic concerns the data management issues associated with RFID technology in the supply chain and the subsequent increase in volume of data for the company (Angeles, 2005).

The volume of data inflows needs to be addressed to ensure security of the information. A possible solution to the data volume management issue comes from companies that are searching for better ways to share and manage large amounts of data – example data grids. Forward-thinkers imagine data grid systems that connect large numbers of enterprises, entire supply chains, and customer bases in order to manage large amounts of information effectively (Thibodeau, 2004). The data management and volume

management concerns relate to possible infrastructural issues with the increase in RFID data, and securing large amounts of information could be very challenging in the global supply chain.

The Entrust white paper discusses data privacy issues and the consequences of failure to comply with data/privacy protection laws (Entrust, 2004). An example would be the failure to comply and provide privacy, audit and internal controls could result in penalties ranging from large fines to jail terms. Compliance with regulations and standards is a concern that every organization must deal with and also whether or not the other members of the supply chain are adhering to them as well. Some examples of information security regulations for organizations to familiarize themselves with are: Sarbanes-Oxley, the Gramm-Leach Bliley Act, the European Data Privacy Directive, and the Basel II accord. (Pironti, Unisys)

Current information security trends, mentioned by the Information Management Journal (2004), are the increase in the percentage of information security budgets among companies and a decrease in the records lost or damaged among companies. These trends show promise that securing information flows from a generic organizational perspective are gaining more attention from companies.

The general ideas, in Lee and Wolfe (2003), are that e-marketplaces are still in the early stages of their development life cycle. E-marketplaces are creating more complex supply chains that are requiring more complex information and data security across the chain. Securing information across the global supply chain is uncharted territory, but the

need for it is gaining momentum and as more literature on the topic is coming to the forefront, organizations will be better able to understand the issues in protecting their information effectively.

It is clear from the surveyed literature that the importance of securing information is well recognized within an organizational setting. However, information security in the context of securing critical information flows between and among organizations has received no attention and, in particular, information security in the supply chain has received scant attention. Even in the area of information security within a single organization, no studies and/or concept papers appear to exist documenting the need for developing a strategy to deal with threats to the information critical to the functioning of the organization.

Interorganizational information flows are a direct consequence of the ubiquitous use of the Internet and its communication protocols and the explosive growth in business to business (B2B) E-commerce. Clearly there is a significant gap in the research literature on inter-organizational information security. The research literature does not appear to have dealt with the underlying area of inter-organizational information flows and the issues that drive the management of such flows, leave alone deal with the component issue of security in the context of inter-organizational information flows.

Also clear from the literature survey is the scant attention paid to this developing area, especially in the management of supply chain information security, at the corporate level. There is clearly a need for developing the procedures and protocols for establishing a strategy to secure information in the supply chain, which includes other organizations

as well. While related to this lack of attention to supply chain information security (SCIS), it is still disturbing that there does not appear to be any literature on ways to deal with the introduction and control of emerging information technologies in the supply chain, especially across multiple organizations.

One of the critical issues, in the smooth functioning of inter-organizational alliances and cooperative ventures, is one of power and control in the B2B relationship. It is not surprising that no attention appears to have been paid in the research literature to this topic in the context of SCIS.

Given the nature of many multi-organizational supply chain relationships, we are encountering, especially in manufacturing industries, an increasing number of global supply chain affiliations. Information flows across such a supply chain are far more distributed and less controllable by one organization. Local mores, ethics, accounting practices, financial service rules, currency and stock markets, governmental control, privacy legislation etc. are all likely to influence the supply chain. These and other parameters add many layers of complexity to the management of information flows in the trans-border supply chains of today, which are only likely to expand in the era of virtual organizations already on the horizon.

Discussion

This section will focus on the issues related to information flows across corporate boundaries. Specifically, we concentrate on the need to identify: information control and security issues, infrastructural issues, strategy development parameters and issues, local

protocols, emerging technologies impacting the flow of information in the supply chain, power and control in inter-organizational systems and its impact on information security, security of "transshipment" points of both data and materials, and security of accounting and financial transactions.

Infrastructural issues:

The supply chains of today are typically multi-organizational and across different countries. Even with a single organization involved in the area of information security, the infrastructure of the organization would be an issue in the securing of information. Not that this area is all that well studied in the research literature, it is more an imperative to study infrastructural issues in SCIS in the multi-organizational setting, on account of the stakes involved and the potential for massive disruptions spanning multiple organizations, and even nations.

One aspect of infrastructure likely to affect SCIS in the multi-organizational context is the type of organizational structure that is to be found in the organizations across the supply chain. Hierarchical structures would appear to lend themselves more easily to control and, hence, security of information flows through the chain. The trend in most industrialized nations is, however, to have more of a matrix organization and even a flat organization, thus placing a premium on effective communication across the structural span. However, it is unlikely that organizational participants in the supply chain have similar organizational structures, let alone the same structure. Also, the level of technological sophistication and the ability to deal with disruptions and security breaches are likely to be all over the spectrum.

The flexibility of an organization, the learning orientation and responsiveness of its workforce to information flow disruptions in the supply chain are likely to be significant contributors to the reliability and smooth functioning of the supply chain. The presence or absence of well-established communications protocols within the supply chain to handle information flow disruption would, surely, impact the supply chain's functioning. The human aspect is very critical in the securing of information flows.

Humans are likely to be the most important on both sides of this equation; namely, they are likely the perpetrators of SCIS violations and they have to be the ones to prevent it and/or fix these problems. The level of sophistication and trustworthiness and training required by organizations, in the supply chain, of their information processing employees, and their technical competence would all play a role in securing the information flows in the supply chain. Further, given the collective nature of the job of securing the information flows across organizational and national boundaries, well established mechanisms must be developed for information sharing across organizations in the supply chain and for promoting inter-organizational learning.

Strategy development

It is questionable whether there exists a well thought out strategy for securing information flows even in a single organization setting. Often the operational practices put in place by the Information Technology infrastructure passes for "strategy" in this

regard. Such a practice in the world of the global supply chain in securing information flows is not only bound to fail but also is likely to prove very perilous for ensuring the safety of both information and materials flowing through the supply chain.

We are talking about the need, here, for the formulation of a well thought out, multi-organizational, multilateral strategy for securing information flows in the global supply chain. One aspect of this area of strategy development is likely to be the development of a process for diversifying SCIS strategy across the chain and bridge the gaps that would exist between and among the individual organization strategies, when set up, and the multilateral strategy needed.

This multilateralism is likely to evoke the specter of power and control in the supply chain. It would then become necessary, as part of the process of protocol development, to deal with power and control issues in an acceptable way for the sake of the larger good of the chain as a whole. This is likely to be a thorny problem, requiring much tact and diplomacy on the part of the leadership of the organizations in the supply chain, especially those, organizations and personnel that are considered the most influential.

One factor affecting the development and implementation of a strategy for SCIS would likely be finances. It is very unlikely that the financial burden of securing the information in the chain will be equally shared by all parties in the chain irrespective of their size, ability to pay, and gain from the extent of use of the information. Also, procedural and infrastructural individualities related to organization structure, cultural

setting, governmental regulations, infrastructure, and size will all likely shape and mold SCIS strategy.

Local protocols

Study of information flow security in a trans-border, multi-organizational supply chain is a necessity stemming directly from the scope of such chains and the opportunities for its disruption based on a variety of factors. One such factor would be the protocols and practices local to the organization in its setting, typically abroad. We have already alluded to the need for inclusion of financial aspects in SCIS strategy formulation. The financial practices that are local to the organization setting, in terms of expected ROI, cash flow requirements, debt service and ability to incur debt etc. will all play a role in determining both the operation and management of the information flows in the chain. Additionally, accounting standards differ widely across the world. Short of imposing a common, US like, FASB orchestrated standard, awareness and accommodation of the diversity of accounting practices becomes an imperative for securing, especially financial, information in the chain. In addition, there has to be responsiveness, in the SCIS strategy, to legislative mandates, such as Sarbanes-Oxley, in ensuring compliance at least in the countries with such legislative priorities.

Local cultural practices may eliminate or exacerbate security breaches. To an extent, the practice and management of information security is based on a trust no one attitude, which is likely to clash with the accepted cultural norms in some environments. Similarly, some locations in the chain are far more likely to be physically more secure than others. Clearly, physical security of information assets is a first step in ensuring

overall SCIS. Since there are significant cost and capacity overheads that attend on practices such as encryption, the level of security through the chain is unlikely to be uniform and of a suitably high level. The challenge then will be to develop not only acceptable practices, but also to develop a strategy that is sensitive to local issues in ensuring that the weakest link does not end up compromising SCIS across the chain. The infrastructure, especially with regard to data communications, around the world and in different business organizations is far from uniform. Add to this the prevalence of ancient laws and modern regulations, and what we have is the making of a nightmare scenario of having communication barriers within the chain for the sake of shoring up one or more weak links in the area of SCIS.

Emerging technologies

The emergence of new wireless networking technologies such as Blackberry, wireless enabled PDAs, ad-hoc networks, and RFIDs has introduced a new twist into the dialog on information security that is becoming more urgent by the day. The frustrating aspect of dealing with securing these technologies is likely to be the wide variation in both standards and infrastructure across organizations in the supply chain. RFID technology, hailed as the next best thing to sliced bread, has been embraced with open arms without regard to the infrastructure needed to make information flows in this context secure. RFID tags are not tamper proof. Also, they can be removed and replaced by mischief minded hackers. Encryption would only partially prevent sabotage of RFID based information flows.

In this environment of rapidly changing technologies and expectations, it may be necessary to layer security systems and allow for layered handling of data and

information in a secure fashion appropriate to the information being handled. The greatest challenge is likely to be the necessity to have all participants in the handling of information flows in the supply chain to have an acceptable level of security in the use of emerging technologies in the supply chain, even if they are not using them, as yet. This mandates the need for development of a SCIS strategy that includes the securing of information handled and flowing through emerging technologies.

Power and control issues

Smooth functioning of a supply chain, and especially one that spans multiple organizations across national and cultural boundaries, is predicated on successful relationship management within the chain. While individual organizations may emerge as leaders in the management of the supply chain, coercive practices are unlikely to work effectively in this environment. Securing information handling, and information flows, in this environment is but a piece of the overall relationship management puzzle, albeit a very important one. It is only now that researchers are beginning to turn towards relationship management issues in B2B E-commerce and, tangentially, the supply chain (Li et al, 2004). It is not clear that ones who control the relationship will or should automatically control SCIS. In the perspective of power and control of the supply chain relationships, SCIS would appear to play a role in the determination of the overall strategic posture to be adopted by organizations, individually and collectively, in managing the supply chain. It has to be that organizations, especially large and used to getting their way, have to become more flexible in the collaborative that is the supply chain, so as not to win many battles only to lose the war.

It is arguable whether the same parameters would attend relationship management

irrespective of organization size and contribution to the chain. Further, given the diversity of locations and protocols, not to speak of legislation and legislative priorities, it is even more unlikely that one size would fit all, in terms of establishing either guidelines or checklists for successful relationship management and, hence, SCIS management.

There are many relationship layers within the supply chain. The issues that impact supplier-to-supplier relationships and SCIS management are likely to be different from those that impact vendor-supplier and vendor-vendor relationships. Infrastructural capabilities in these relationships are likely to be significantly skewed in favor of large vendors as opposed to small suppliers and, yet, the success of SCIS management is likely to depend on how well the skewed relationships are managed. It may be necessary to educate, on a continuing basis, the smaller, seemingly less significant, players in the chain to the pitfalls of lax security along with the procedures, and the necessity there for, to avoid security compromises. Again, the security system is going to be only as strong as the weakest link, and the mindset of the bigger players has to change to accommodate this reality to ensure smooth functioning of the supply chain.

Research Issues/Opportunities

It is evident, from even a cursory glance at the content of the previous section that a vast array of unresearched areas exists on the topic of SCIS. Some of it, clearly, has to be dealt in tandem with the generic areas such as relationship management and some with the trans-border data flow areas. The typical research methodologies on business practices await business developments and are post-facto. What is needed, immediately,

is fact-finding type of research that leads to the development of a conceptual model encompassing all aspects of the SCIS spectrum. This perspective leads us to suggest, chronologically, the following research steps in answering some of the salient research questions framed thus far in the article.

- Develop case studies to identify examples illustrating the issues highlighted and organizational response, if any. Specifically,

    - Examine the workings of global supply chains with a focus on identifying presence and absence of SCIS practices. Document consequences of action, inaction, and misaction.
    - Identify, in a case study setting, relationship management issues that impact SCIS
    - Identify, through case studies, the security practices and security breaches in the handling of information flows by intermediate trans-shipment points on the Internet used by supply chains.
    - Identify, through case studies, the procedures or the lack thereof, in the area of strategy formulation, aimed at SCIS.
    - Identify trans-border parameters of impact in different supply chain environments, through case studies.

- Develop case studies/field studies to identify infrastructure capabilities and limitations in handling security issues in inter-organizational information systems in the supply chain. Specifically,

    - Identification of multi-organizational data base security issues and

responses

- Security of data communications in the supply chain across organizations
- Development of protocols and procedures for identification of and the upgrading of the weakest link in the inter-organizational supply chain
- Training and retraining of personnel dealing with the multi-organizational information and material flows
- Organizational learning issues and development of monitoring mechanisms for securing information flows in the supply chain

- Based on the case studies and the field studies, development of a comprehensive model for securing inter-organizational information flows in the supply chain, to include:
  - Evaluation of emerging technologies from a security perspective
  - Development of infrastructure
  - Handling of legal and cultural issues
  - Organizational learning in the inter-organizational information security context
  - Strategy formulation and alignment
  - Strategy Implementation

References

Angeles, Rebecca .(Winter2005), "**RFID Technologies: Supply-Chain Applications and Implementation Issues.**" ***Information Systems Management***, p51, 15p

Barry, Christopher. January 2005, "**RFID tracks packages, 'speaks' to consumers: smart packages not only improve supply chain management- they ensure product security, authentication – Emerging Technology**".
Source: http://www.findarticles.com/p/articles/mi_m0UQX/is_11_65/ai_812...

Coffee, Peter *(*12/13/2004), "**Security is a moving target**." ***eWeek***; Vol. 21 Issue 50, pD1, 4p

Hale, John C.[1] john-hale@utulsa.edu, Landry, Timothy D.[2,] tlandry@ou.edu ,Wood, Charles M.[3] charles-wood@utulsa.edu. May/Jun2004, "**Susceptibility audits: A tool for safeguarding information assets**." ***Business Horizons***; Vol. 47 Issue 3, p59, 8p

Lee, Hau L., Wolfe, Michael. Jan/Feb2003, "**SUPPLY CHAIN SECURITY WITHOUT TEARS**". ***Supply Chain Management Review,*** Vol. 7 Issue 1, p12

Murtaza, Mirza B.; Gupta, Vipul; Carroll, Richard C. 2004, "**E-marketplaces and the future of supply chain management: opportunities and challenges**", ***Business Process Management Journal***, Vol. 10 No. 3, pp.325-335

Pironti, John P. "**Securing Information Infrastructure: Expert Advice on Evaluating the New Risks and Structuring Your Defenses**." Source: ***Unisys*** (Whitepaper), 8p

Reddy, Ram. Nov. 2004, "**Without Safety Nets: Will Super-efficient supply chains take one beating and fail to keep on ticking**?." Source: ***Intelligent Enterprise*** http://www.intelligenteai.com/showArticle.jhtml?articleID=51201670

Source #1: Entrust (Whitepaper) September 2004, "**Protecting Your Most Important Asset: Information – How Data Security Mitigates Risk and Enables Compliance**". Entrust Publication, 10p. www.entrust.com

Source #2: ***The Information Management Journal***, Nov/Dec. 2004, "**Businesses Improve Cyber Security**".

Thibodeau, Patrick. 4/5/2004, "**Data finds a place on the grid**." ***ComputerWorld***, 00104841, Vol.38, Issue 14

Wagner, Raymond, 2003 "**Secure the incompatible**." ***Computer Weekly***, 00104.

Willoughby, Mark. Dec. 20, 2004, "**Securing RFID Information: Industry standards are being strengthened to protect information stored on RFID chips**." ***Computer World***

Li, X., Kunnathur, A. S.,T.S. Ragu-Nathan, T. Jitpaiboon, "**Learning Capability, Supportive Leadership and Power in IOS Context**," Proceedings of the ***National DSI Conference***, Boston (2004)

Zhen, Jian. 1/5/2005, "**The war on leaked intellectual property**." Source: ***ComputerWorld*** Article Quicklink# 51749787, 11/18/2003