Global supply-chain securization as applied to seaport operations: A knowledge-based approach

Charles-Henri Fredouet *

Abstract

Organizations, would they be individual companies or large multi-firm networks, face a wide variety of potential risks requiring dedicated keen management. It all the better applies to supply-chains as risk, related to both physical and information flows, pervades the whole logistics network and has acquired a new and growing security dimension since 9/11. More specifically, as they are now under the permanent threat of terrorism, and because offering sufficient security levels is bound to become a necessary condition for global supply-chain membership, seaports need to adjust their risk management strategy and processes accordingly. In such a context, this paper aims at describing the project of a decision-support system, dedicated to container transit security-wise decision making and which features an expert-system architecture.

Keywords: decision support systems, organizational performance, logistics networks, seaport management.

1. Introduction

Until recently, transportation risk management has mostly dealt with either natural or accidental man-made disasters focusing predominantly on incident prevention and consequence mitigation (Merrick et al., 2002). Since the 2001 9/11 tragedy transportation operators, as well as shippers and public authorities, have become aware of a new type of risk, still man-made, but this time intentional (Abkowitz, 2003).

*ISEL, Le Havre University, quai Frissard, BP 1137, 76063, Le Havre cedex, France. E-mail: chf@univ-lehavre.fr
Securing the global supply-chain has thus become an important concern for governments, practitioners and academics, and all the more so as:

1. beyond terrorism-related risks, lie numerous other intentional man-made transportation risks such as drug smuggling or tax avoidance; and
2. in a widely spread time-based competition context, securing supply-chain operations should not be sought at the expense of delay efficiency in physical and informational flow processing.

Since 2002 various initiatives have been launched to that end by such public institutions as US Customs and Border Protection (CSI), European Union (Custom Security Program) or International Maritime Organization (ISPS).

Academics and practitioners have also begun addressing this topic. A review of supply-chain risk management literature shows that security risk is dealt with mostly as a supply-chain disruption issue, and using the traditional three-step risk management process: risk identification, risk assessment and risk hedging and mitigating.

Among all possible contributions to this trend, involving multiple stakeholders at the crossroads between local border protection and global supply-chain performance, stands the design and implementation of relevant decision support systems. Consequently, a project of this type has been launched, dedicated to securing seaport supply-chain links. Following a field data collection case-based methodology, calling upon specific process and risk analysis resources, the project leads to a knowledge-based system, well-suited for the modelling of the ill-structured patterns shown by risk management decision processes. Section 2 resets these processes within the frame of organizational risk management and section 3 illustrates how they can be used in, project presentation with reference to seaport centric security handling within logistics networks.

2. Organization risk management

In the introduction of his book on risk modelling, assessment and management, Haimes (2004) insists on the fact that the more complex a subject is, the less one knows about it, and the less one knows about a complex subject, the more imperative is the need for risk assessment and management. More specifically, would they be private or public, for profit or not-for-profit, socio-economic organizations are complex by nature. They may therefore have reached a wide variety and high levels of risks, requiring dedicated management. Risks likely to be encountered by an organization need be identified (section 1), before entering into some detail as to how organizational risk is managed (section 2).

2.1 Identifying organizational risks

Organizational risk is defined by Barton and others (2002) in a report from the Institute of
Internal Auditors as; any ‘issue, threat, or action which could impact a company’s ability to meet its business objectives and execute its strategies successfully’: Such a definition allows for great diversity in the nature and various other characteristics of organizational risk. This diversity has been addressed by academics through a number of different approaches, which can be structured along two dimensions:

1. the object of the approach, either the risk itself or one of its characteristics; and
2. the orientation of the approach, either horizontal, aiming at classifying, or vertical, aiming at deepening.

As applied directly to organizational risks, the classification features a **financial risks** category, within which risks are due predominantly to the volatility of interest rates or exchange rates, but also to situations of asset-liability mismatch. Because all organizational risks are not financial, the classification, therefore, adds other categories as outlined by Vedpuriswar and others (2003):

- **hazardous risks**: “[which] refer to natural hazards, accidents, fire, … that can be insured”;
- **operational risks**: “[which] cover systems, processes and people, [including] issues such as […], human resources, information technology, […]; and
- **strategic risks**: “[which] stem from an inability to adapt to changes in the environment such as changes in customer priorities, competitive conditions and geopolitical developments.”

Other classifications deal with the specific characteristics of organizational risks. For instance, Christopher and others (2003) have categorized risk drivers into four levels from which they may operate:

- Level 1: *Process/Value Stream*, where risks “[arise from] poor quality, sub-optimal supply-chain performance, demand volatility and shifting marketplace requirements”;
- Level 2: *Assets and Infrastructure Dependencies*, where risks “[arise from] the loss (temporary or otherwise) of links, nodes and other essential operating assets”;
- Level 3: *Organisations and Inter-organisational Networks*, where risks “[arise from] business strategy and microeconomics, one of the most widely recognized sources of supply-chain risk [being] the failure of a single source supplier”; and
- Level 4: *The Environment*, where risks “[arise from] the wider macroeconomic and natural environment of the organization, […], factors [being] political, economic, social, and technological elements of the operating and trading environment, as well as natural phenomenon – geological, meteorological and pathological.”

Within the organizational risk-centric literature there is a need to go beyond classification and gain better knowledge of a given risk characteristic. Following this line of research, and in a business context characterized by the growing importance of the network dimension of organizations, a number of academics have recognized what appears to be a key dependency
relationship by linking this dimension to organizational risk’s levels of probability and magnitude (Sutton, 2006). These higher level observations are that:

- **the network is more homogeneous**, a risk for one component of the network being also a risk for (many) others; conversely, heterogeneous networking improves network defense capabilities, as network vulnerability is reduced to the degree to which critical activities are separately led by differentiated components (Zhang et al., 2001).
- **the rhythm of change** in a network’s design or control/operational processes is faster, as an organization is especially vulnerable during the transition phases between one stage to another (Haywood and Peck, 2004).
- **the network features more interactions** between its components (‘interactive complexity’) and more interdependencies between its functions (‘tight coupling’), thus facing the risk of a major accident resulting from the propagation of an initial minor incident (Perrow, 1994).

Finally, producing new knowledge on a given type of risk is definitely the key focus of interest among academic researchers in the field of organizational risk management. More specifically, the concern is with:

- **ecological risks** (Beer, 2006; Hoffman, 2005; Stead and Stead, 2004; Willis et al., 2004; Power and McCarty, 2002),
- **project risks** (Chapman and Ward, 2003; Pich et al., 2002; Barki et al., 2001; Ward, 1999),
- **IT/IS risks** (Tafti, 2005; Bhattacharya et al., 2003; Suh and Han, 2003; Blakley, 2001; Finne, 2000), and
- **supply-chain risks** (Handfield et al., 2006; Papadakis, 2006; Bensoussan, 2006; Johnson, 2006; Juttner, 2005).

These academic contributions have been augmented by individual and collective contributions on risks from practitioners. This experience on a variety of potential risks facing, organizations, irrespective of whether they are individual companies or large multi-firm networks, is available to them for designing and implementing efficient and effective risk management programs.

### 2.2 Managing organizational risks

The design of a management system dedicated to a given set of risks is a two-step process: the first step is the selection of the risks to be managed; and the second step is the actual design of the risk management system:

**Selection of risks to be managed**

Selecting risks to be managed is, in itself, divided into two successive stages: one consists in the identification of the manageable risks met by the organization; the other leads to the
specification of the risks that the organization will actually manage. Besides Sadgrove (2005) relevant questions on the relative importance, likelihood and impact severity of such risk for a given organization, the design of this two-level decision process, as described by Lo (1999) in a financial risk management context, may refer to the 3P’s of Total Risk Management: *preference* for a risk rather than for another; *price* to be paid to hedge a risk; and *probability* of a risk to occur. In the present, more general, context, preferences may intervene at the risk taking identification level, whereas prices and probabilities may be considered at the risk managing specification level within the risk selection global process:

- **Risk taking identification level**: some risks are definitely not incurred by an organization; some others are effectively incurred by, but unknown to, the organization; finally, some are voluntarily avoided by the organization, as not in its set of strategic risk preferences; obviously, these three risk categories are out of the scope of risk management system design. Conversely, some incurred risks are definitely unavoidable by the organization, because they are naturally inherent to its activities; some other risks are deliberately and consistently taken by the organization, following its own strategic risk-preference rationale; this time, these two risk categories may make for the design of a dedicated risk management system.

- **Risk management specification level**: once risks met by the organization are defined, a decision has to be reached as to which will be managed: facing a given risk, the organization may decide neither to try to avoid it nor to try to reduce its unwanted consequences; in some other risk setting, it may, on the contrary, decide to invest heavily in risk hedging and risk mitigation activities. The probability of actually incurring the risk, the degree and nature of the risk’s impact on the organization, and the cost of hedging and/or mitigating the risk, are among the most important factors to be accounted for in this decision process (Table 1):

<table>
<thead>
<tr>
<th>Decision factors</th>
<th>Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk probability (P)</td>
<td>H H H H L L L L</td>
</tr>
<tr>
<td>Organizational damage (D)</td>
<td>H H L L H H L L</td>
</tr>
<tr>
<td>Risk management cost (C)</td>
<td>H L H L H H L L</td>
</tr>
</tbody>
</table>

*Note: H = High, L = Low*

### Design of risk-management system

Following the selection of the risks to be managed, the risk management system may be designed to support a three-phase decision process: risk identification, risk assessment, and risk treatment (Barton *et al.*, 2002):
• The risk identification phase needs initially to describe the characteristics of the potentially risky situation by identifying a set of indicators. Then, a dedicated information system has to be established to collect data on these indicators, from existing or to-be created, automated or not, data sources, on a batch or real-time mode of transmission (Lee and Whang, 2005).
• The risk assessment phase builds upon the formerly created and fed data base, to help validate the actual existence of the monitored risky situation, and estimate the probability of risk occurrence and that of risk consequences, as well as the magnitude of these consequences (Lupton, 1999).
• The risk treatment phase encompasses all risk hedging and/or risk mitigating activities. This phase is very knowledge-intensive, as solutions to prevent, or to optimize the response to, a given risk, draw heavily on regulation, technology and experience. Actually, a growing number of companies use knowledge management processes and tools for risk-management purposes, giving rise to what Neef (2005) calls the KRM (knowledge and risk management) perspective.

This whole risk management process may obviously be quite difficult to design and implement. It all the better applies to supply-chain risk management as not only do the levels of local and global integration get higher within logistics networks, but also this risk has acquired a new and growing security dimension since 9/11.

3. Logistics networks risk management

For a global supply-chain, it has of long become a necessity, to outperform its rival organizations, to offer shorter delays and better quality, while at the same time remaining cost-effective and flexible. More recently, a supply-chain’s set of performance criteria has been enlarged to include security, following the development of trade globalizing, activity outsourcing and lean manufacturing strategies. Security risk management appears, therefore, now as a key and desirable performance factor in global logistics networks. Initially the security handling issue in global supply-chain is discussed before focusing upon the securization of the seaport link, probably the most vital link in today’s internationally extended supply-chains.

3.1 Handling security in the global supply-chain

Actually, so-called supply-chains are networks of actors dedicated to customers. Risk, related to both physical and information flows, pervades the whole logistics network:

• at each node, not only a distribution center, a manufacturing or assembly plant, but also an airport, a maritime port or data storage and processing center (Goossens, 2004; Tatsiopoulos et al., 1999; Einarsson and Rausand, 1998);
• along each link, involving the movement of either physical goods in mono-modal or multi-
modal (road, rail, sea, air, inland water) transportation activities, or information in mono-modal or multi-modal (digitized, mail, fax, phone) transportation activities (Dobbins and Abkowitz, 2002; Bandyopadhyay et al., 1999).

Supply-chain risks may arise from any of the three supply-chain’s design, control and operation sets of phases:

- **Design-wise**, risks may stem from the decisions taken when trying to optimize the supply-chain both as a global process (structuring activities following a speculation/postponement-based strategy; allocating resources through outsourcing/offshoring decision-making) and a global network (selection of logistics sites; and transportation modes);
- **Control-wise**, risks may stem from the processes of setting goals (supply-chain planning), coordinating operations (supply-chain execution) and/or reporting activities (supply-chain performance measurement).
- **Operation-wise**, risks may stem from the everyday manufacturing/assembly (production network) and warehousing/transportation (distribution network) sets of activities, applied to physical and informational products or services, and as conducted by manufacturers, retailers and logistics service providers.

Following the distinction, made among supply-chain risks by Kleindorfer and Saad (2005) between those arising from the problems of coordinating supply and demand, and those arising from disruptions to normal activities, such design-, control- or operational-born risks may for some of them be described in traditional terms of cost, quality, flexibility and delay:

- **cost-typified risks** may be due to too many distribution centers or DCs (supply-chain design), inappropriate cost-calculation method (supply-chain control) or unexpected material cost variation (supply-chain operation).
- **quality-typified risks** may be due to supplier performing under expectations (supply-chain design), no product/process traceability (supply-chain control) or inaccurate order preparation (supply-chain operation).
- **flexibility-typified risks** may be due to excessive activation lead time of the transportation mode (supply-chain design), excessive re-estimation lead time of the planning information system (supply-chain control) or excessive processing lead-time of customer orders (supply-chain operation).
- **delay-typified risks** may be due to misplaced speculation versus postponement of the global process (supply-chain design), a defective operational synchronization system (supply-chain control) or lengthy customer delivery delays (supply-chain operation).

---

1For supply-chain risks classification, see Bailey and Thomas (2004), and also Ziegenbein and Nienhaus (2004), who have derived from the Supply-Chain Council SCOR™ model. A classification identifying Planning and Control risk (SCOR’s PLAN), Supply Risk (SCOR’s SOURCE), Process Risk (SCOR’s MAKE) and Demand Risk (SCOR’s DELIVER), plus a fifth category, this time not borrowed from the SCOR model, dedicated to all so-called “environmental” risks.
In addition to those cost-, quality-, flexibility- and delay-related supply-chain risks, the supply-chain security risk has attracted growing interest, especially since 2001: Logistics networks are complex organizations that exist under always heavier constraints of efficiency (generally measured in terms of customer service, of which delay is a predominant component) and effectiveness (generally measured in terms of cost).

But, as Christopher (2003) states in his practical guide to creating resilient supply-chains, “the adoption of lean and agile practices has made [supply-chains] increasingly reliant on the existence of a reliable, secure […] communication, transport and distribution infrastructure.” More generally speaking, supply-chains can be deeply upset by any disruption in the flow of goods and/or information that they handle.

Such disruptions are categorized into six failure modes by Sheffi and others (2003): disruptions in supply, disruptions in transportation, disruptions at facilities, freight breaches, disruptions in communications and disruptions in demand. They become increasingly likely, with the advent of new sources of threat for logistics organizations, among which terrorism is obviously the most dangerous: “until recently, the approach to transportation risk management assumed that when man-made disasters occurred, they were accidental in nature and not due to malicious intent. Terrorist activities, culminating with the tragic events of September 11, 2001, have dramatically changed this landscape” (Abkowitz, 2003).

Apart from measures aiming at improving local and global resiliencies within the logistics networks, processes (combining dedicated activities and associated resources) have to be implemented to ensure the best possible level of supply-chain security in this potentially highly risk context. Beyond traditional asset protection, supply-chain security management must, therefore, address process integrity issues defined as “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 of unauthorized contraband, people, or weapons of mass destruction into the supply chain” (Closs and McGarrell, 2004).

In designing such processes, one must be aware of the necessity of a two-sided global approach:

- on one side, improving supply-chain security should not be sought after without considering other logistics performance criteria. Cited by Hannon (2002), S. Zujkowski, then senior vice-president of Savi Technology, warned that by implementing security-intensive control processes, ‘we risk achieving the same outcome the terrorists desire [which is] to bring our economy to a standstill’. Although from a far less pessimistic standpoint, it may also be said that, in some instances like hazardous goods transportation, storage and transformation activities, where physical activities are an important part of security measures, reaching better supply-chain security may obviously result in higher costs and/or longer delays. However, thus drawing from past Total Quality Management (TQM) successful experiences (Lee and Wolfe, 2003), all security-wise risk management innovations and initiatives, brought by public authorities and private companies since 2001, have been designed to combine supply-chain security and trade facilitation. Hailing the ratification of the WCO (World Customs
Global supply-chain securization as applied to seaport operations: A knowledge-based approach

Organization) Framework of Standards, Th. Fletcher, Vice-President Supply-chain Compliance, Security and Diversity, for IBM Corp. reminds us that “besides improving the security of our trade lanes, the Framework offers […] efficiencies derived from a common global process, cost reductions and supply-chain resiliency”. The way to such national and international supply-chain security risk management programs has been paved by the well-known International Ship and Port facility Security code (ISPS), Container Security Initiative (CSI), Customs-Trade Partnership Against Terrorism (C-TPAT) and Smart and Secure Trade lanes (SST), in which informational, more than physical, activities also form the core of security measures.

- the other side of supply-chain security risk management’s global approach pertains to the necessity of conducting integrated risk management system’s design and operation in a collective rather than individual manner:

Governments and international governing bodies take care of national security issues through border protection measures and look for ways to financially support the security of international supply-chains (Dulbecco and Laporte, 2003), but also promote trade facilitation operating standards such as the Authorized Economic Operator (AEO) status.

Within these institutional frameworks, companies have to devise their own risk management systems: “every supply chain and every company should identify the most effective and efficient way to protect itself” (Sheffi et al., 2003). However, doing so, they need to take into account the impact of their belonging to extended-enterprise systems as: “business risk becomes highly dependent on business partners rather than being a largely internally controllable and monitorable item” (Sutton and Hampton, 2003).

Under these two global-minded constraints, the design and operation of supply-chain security risk management systems adopt the standard three-step scheme of risk identification, risk evaluation and risk hedging/mitigation. At each step, various tools have been developed, including qualitative-based (Bass and Robichaux, 2001) or quantitative-based (Dey, 2001), those dedicated to industrial (Einarsson and Rausand, 1998) or transportation (Huang et al., 2004) sectors, and those addressing physical (Hopkins et al., 1999) or informational (Sharma and Gupta, 2002) flows risk management issues.

More specifically, along the international supply-chain, seaports appear to be natural heavily-loaded security-risk links: through seaports, a wide variety of goods are imported/exported in large volumes from/to numerous points of origin/destination, each physical flow being accompanied by a complex and, only partly digitized, flow of information; multiple and growingly sophisticated activities and resources are involved in the physical and informational flow management processes, both within the seaport link and within the immediately preceding and following supply-chain links.

Given they are now under the permanent threat of terrorism, offering sufficient security levels is bound to become a necessary condition for global supply-chain membership, seaports need therefore to adjust their risk-management strategy and processes accordingly, with the help of dedicated decision support systems (Harrald, Stephens and Van Dorp, 2004; Van de Voort et al., 2003).
3.2 Securing the seaport link SEAPORT

As with any other organization, a seaport community may improve its risk management following two non-exclusive generic ways: one, the safety way, is to upgrade its risk resiliency capacity, that is its ability to deal with, and recover from, a risk having actually occurred; the other, the security way, is to enhance its risk avoidance capacity, that is its ability to prevent a risk from actually occurring.

From a security standpoint, the main issue for seaports involved in international supply-chains may most likely have been summed up by Willis and Ortiz (2004) in a technical report from Rand Corp.:

Actions to ensure the security of the system of containers and their conveyances have traditionally focused on preventing smuggling and theft. Since September 11, 2001, supply-chain security has been redefined as preventing terrorists from targeting the containerized supply chain or transporting a weapon in a shipping container. The change in focus raises questions about the effectiveness of proposed security efforts and the consequences they may have for supply-chain efficiency.

In such a context, where optimizing the compromise between operational security and facilitation may generate substantial competitive advantages for seaports, the combined objectives of a relevant decision support system are therefore:

1. to help seaport operators prevent anything identified as (potentially) risky to enter, and a fortiori leave, seaport’s functional limits; and
2. to ensure sufficient security performance while at the same time contributing to, rather than hindering, other especially cost- and delay-related performance improvement programs (Richardson, 2004).

The decision support system project proposed hereafter has been launched in this context and with this two-fold ambition. It comprises the development of a knowledge-based software platform, dedicated to collecting data on critical risk indicators for all shipments bound for the seaport supply-chain link, and the timely provision from risk management expertise, the requisite information on delays necessary for the operators involved, to optimally deal with the risks potentially associated to each of these shipments.

This project features a three-stage global design methodology: firstly, it describes the processes to be secured; secondly, it performs risk analysis on these processes; and thirdly, it builds the resultant decision support system.

- The processes described pertain to informational as well as physical flows; they are led not

---

2Functional limits include all the processes which the seaport community is entrusted to optimally manage, and therefore secure, by its global supply-chain partners.
Global supply-chain securization as applied to seaport operations: A knowledge-based approach

only by port operators between the pre-defined points of entry to, and exit from, seaport link boundaries, but also by members of the other logistics networks involved in the supply-chain links immediately preceding the seaport. Within the proposed project, only those processes that deal with containerized export shipments are taken into account.

Two reference models, in the field of the optimization of logistics networks, are implemented for the purpose of process description: the ABM (Activity-Based Management) model, dedicated to the processes involved in organizational activity structuring and resource allocation, and the Supply Chain Council’s SCOR® (Supply-Chain Operations Reference) model, dedicated to process analysis and performance measurement. Methodologically speaking, the retained approach is monographic: in a short list of export processes selected for their security-wise typicality, each is described in the level of detail requested by the following step of risk analysis.

- While benchmarking for a risk-centric frame of analysis, and, notwithstanding available specific supply-chain risk analysis methodologies (Tixier et al., 2002), attention is paid to the Hazardous Analysis and Critical Control Points (HACCP) method so successful in the food industry. HACCP is a risk identification, evaluation and control system based on seven principles:
  1. conduct a hazard analysis;
  2. determine the critical control points;
  3. establish critical limits;
  4. establish monitoring procedures;
  5. establish corrective actions;
  6. establish verification procedures; and
  7. establish record-keeping and documentation procedures.

These principles help formulate the guidelines for the present project’s conduct of risk analysis:

- Identify potential risks in a process by scrutinizing each of its activities and resources.
- Decide which potential risks will be managed, depending mainly upon their probability of occurrence and the severity of their consequences.
- Specify the process point, step or procedure at which the control of each risk may be applied.
- Define the relevant risk measurement indicators to be evaluated at each control point.
- Describe the hedging actions to be taken when risk measures exceed tolerance margins, in order to prevent that risk, or at least reduce it to an acceptable level.
- Establish procedures for periodic and event-driven review, and consequently for possible update and improvement, of the system.

Besides conducting interviews of the supply-chain operators involved to identify their specific risk concerns; as well as looking for supply-chain security best practices, this second stage of the decision support system design methodology requires the setting up of a dedicated inter-
organizational, cross-functional expert team. National Customs, National Coastguards, Federal Immigration Bureau, Federal Police Department and Port Authority’s Safety and Security Department are obvious candidates as members of this team.

- after process modelling and risk analysis, the development of the decision support software platform is based on an expert-system architecture. Because risk management decision processes follow rather ill-structured patterns; their modelling calls therefore on a set of different, but non exclusive, approaches (Vidalis, 2004), within which, together with purely quantitative methods such as genetic algorithms, stands the expertise modelling approach. Already in use for project and concurrent engineering risk management (De Zoysa and Russell, 2003), the expert-system architecture seems also well suited for security risk management. Fitting into the standard frame of decision support systems where an information system feeds required information to a decision process model, it features a data base for the recording of risk characteristics and a knowledge base for the storage of risk management expertise, plus an inference engine for the combination of both contents during actual risk identification, evaluation and hedging operations: in order to optimize container transit security and facility, the expert-system first interprets information on the incoming container, then proposes help for dealing with the shipment (Fig. 1).
A Database on risk-related shipments characteristics has to be fed through real-time traceability not only for goods and transportation means, but also for flows and activities. Such traceability may be obtained from ICT technologies among which RFID, GPS and X-ray devices are the most relevant.

Besides, a knowledge base on risk management is built and then updated by tapping from various local, national and international specialized sources. These sources may obviously be paper, or, more likely now, digitized documents, but also human experts. In this latter case, knowledge acquisition methods have to be implemented, one of which being protocol analysis, well suited for extracting ill-structured, heuristic-intensive decision processes (Ericsson and Simon, 1993).

Finally, beside risk management decision makers, other informational and physical flow operators (shippers, sea-carriers, inland transportation companies, stevedores or clearance agents) may be interested in the information produced by this decision support system.

Therefore, with process-wide risk data communication, multi-sourcing knowledge supply and extended set of potential stakeholders, the proposed project obviously stands at the global supply-chain level. It requires from multiple and varied organizations an implication which may be driven by extending regulation constraints, but hopefully also by the consciousness that security is now fully part of the supply-chain performance model.

4. Conclusion

Socio-economic organizations, whatever their level of complexity, are threatened by a great diversity of potential risks, which they try to hedge and/or mitigate by setting up dedicated risk management strategies and programs. Among all organizational risks, those relating to global logistics networks feature an increasingly important security component.

This kind of risk is partly, but tightly, linked to the widespread threat of international terrorism. Obviously, as gates through national borders and transportation load break points, seaports are therefore highly security risk-intensive supply-chain links, and dealing efficiently with security risks is for them a definite source of competitive advantage in the battle for keeping present, and gaining new spots in global logistics networks.

Actually, properly managing supply-chain security risks has become a necessity for all supply-chain operators involved, all the more so as:

1. security has joined cost, quality and delay in the list of logistics performance criteria favoured by growingly disruption-averse customers; and
2. securing supply-chain operations may at the same time facilitate these operations especially through enhanced process anticipation.

In a move towards improved seaport and supply-chain performance, while hopefully positively contributing to the academic risk management field, this paper describes a knowledge-based decision support system project showing two potentially interesting characteristics: one
comes from the opportunity given to seaport/supply-chain operators and academic researchers to closely collaborate on a mutual advantage basis; the other lies in the opening of further research perspectives, especially in the fields of supply-chain management (performance measurement and physical flow optimization) and information management (interoperability of systems and pattern recognition).

References


Global supply-chain securization as applied to seaport operations: A knowledge-based approach


HACCP, web page, on line at http://www.uky.edu/Ag/FoodScience/FSC540/haccp.html, (as of July 18, 2006).


IMO (undated), ISPS code, web page, online at http://www.imo.org/ newsroom/mainframe.asp?topic_id=583&doc_id=2689 (as of July 18, 2006)


Richardson, M. 2004. Growing vulnerability of seaports from terror attacks, to protect ports while allowing global flow of trade is a new challenge, online at http://www.iseas.edu.sg/viewpoint (as of July 18, 2006).


Supply Chain Council, web site, on line at http://www.supply-chain.org, (as of July 18, 2006)


and Data Systems, 105, 5: 549-560.


