Towards a formulation of a comprehensive risk model for an integrated supply chain: Development of risk interaction and structure constructs

Mario NORBIS
Management Department, Quinnipiac University
Hamden, CT 06518 USA

and

Mary J. MEIXELL
Management Department, Quinnipiac University
Hamden, CT 06518 USA

ABSTRACT

Increasing economic uncertainty, demand instability, and supply interruption from natural and man-made disasters have intensified the frequency and magnitude of supply chain failures. A rigorous analysis and assessment of risk can be difficult to accomplish, however, because of complexities resulting from structure and interaction among supply chain elements. In this research, we contribute to the development of a comprehensive model of risk that considers the vulnerability associated with individual risk elements, along with the structure of the supply chain network, and the risk interactions which may intensify or attenuate individual risk levels.

Keywords: Supply Chain Security, Risk Analysis, Supply Chain Management

INTRODUCTION

Managers have long struggled with the challenges of uncertain events that lead to poor performance in the supply chain. Some of these risk events are routine as late or short shipments from a supplier; others provide major disruptions as in the case of devastating earthquakes that interrupt supply for months or years.

The precepts of risk management are especially pertinent and helpful in this context. Risk is commonly defined as an uncertain or chance event that planning cannot overcome or control. Managers of course are most concerned about risk events that lead to negative outcomes; the risk management process provides a proactive approach that recognizes and manages risks that would impact an organization's success. The risk management process begins with the identification of the possible risk events, followed by risk assessment and analysis where the impact and likelihood of each event is quantified. It is important to determine an appropriate risk response for major risk events which may involve mitigating risk, or transferring or sharing it with a supplier or outside agency. A final step is risk response control, as the risk environment needs to be monitored and updated over the timeframe of the operation.

These principles of risk management readily apply to supply chain management. Indeed, a good deal of research pertaining to the application of risk management to the supply chain has been published over the last decade. A seminal article by Tang [1] defines supply chain risk management (SCRM) as "the management of supply chain risks through coordination or collaboration among the supply chain partners so as to ensure profitability and continuity." Other influential works include Chopra and Sodhi [2] who provide a categorization of risks, and Kleindorfer and Saad [3] who focus on disruption risks. Literature reviews on supply chain risk management include Zsidisin, Ellram, Carter and Cavinato [4]; Rao and Goldsby [5]; and Ritchie and Brindley [6]. There is also a great deal of literature concerning the focused topic of security, nicely summarized in Gould , Macharis and Haasis [7]; and Williams, Lueg and LeMay [8].

This research contributes to this literature by developing a framework for measuring supply chain risk when individual effects, structural effects, and interaction effects are considered. The potential of this approach is demonstrated with an example that includes elements commonly seen in supply chains.

PROBLEM DESCRIPTION

Risk in any organization can be viewed as two-dimensional, i..e. the likelihood of the event occurring, and the impact on the organization if it does occur. Tang [1] provides a classification scheme for the impact dimension, using the term *disruption* to refer to those risks that caused by natural and man-

made disasters such as earthquakes, hurricanes, floods, economic crises, strikes and terrorist attacks. Chopra and Sodhi [2] view risk categories in terms of drivers, and add supplier bankruptcy and single source dependency as additional causes of disruption risk. On the other hand, the term *operational* refers to everyday risks that are driven by uncertainties in demand, supply and cost. Chopra and Sodhi [2] expand on this list by including material delays (e.g. inflexibility and poor quality), information system breakdown, inaccurate forecasts, IP violations (driven by vertical integration and global outsourcing), procurement (e.g. exchange rates), receivables exposure (e.g. bankrupt customers), inventory and capacity mismatches. Much of this operational risk originates naturally as a result of the day-to-day routine that involves the production and delivery of product. There are numerous such elemental, individual risks in a typical supply chain. Thus, we consider two types of risk in this research: operational risk (Type I) and disruption risk (Type II).

The risk likelihood dimension, however, is less well understood. We propose here that the likelihood of a risk occurring may be framed and modeled using three constituents: individual risk element, risk interaction, and supply chain structure. The elemental level consists of the risk events (e.g. late material shipments, labor strikes) to which individual members of a supply chain (e.g. suppliers, carriers, ports) are exposed. These risk elements may be either operational (Type II) or disruption related (Type II). A method for assessing likelihood is frequency analysis, which is useful when an event occurs often enough to provide a reliable estimation. Frequency analysis is not helpful, however, for events that happen infrequently as with many disruptive risks. Later we propose using a systematic benchmarking approach with a focus on best practice in risk mitigation.

The second constituent on supply chain risk likelihood is due to interaction effects between the individual risks, as risk level may be modified through the relationship of elements with other elements of the supply chain. For example, when a trusted, low-risk carrier ships goods from a less well-known and riskier supplier, the trust afforded to the carrier reduces the combination risk of the carrier and supplier together. These interactions are also useful when evaluating the network effect in tightly linked supply chains, as is the case when firms develop partnerships to integrate supply chain processes. Firms in a supply chain are exposed to the risks faced by their suppliers and carriers; for example, a weather-related event that shuts down a supplier quickly shuts down its closely-integrated customer. Both Type I and Type II risks can be influenced by interaction effects in this way.

Finally, the structure provided by the supply chain's design will also affect the overall risk, as individual components of risk will either be increased or decreased depending on the circumstances. A case example for this structural modification of risk may be made when multiple suppliers or parallel carriers are utilized, or when alternative routings are used for international shipments that involve different ports. Again, both Type I and Type II risks can be influenced by structural effects in this way.

Within this framework, we define the research question guiding this effort as follows: how can the overall risk in a supply chain be assessed given (1) the existence of multiple types of risks (i.e. operational and disruption), and (2) the existence of numerous risk elements that interact and (3) the influence of supply chain structure that may increase or decrease these effects.

MODEL CONSTRUCTS

Supply Chain Risk Elements

In this section we discuss risk that occurs at the level of the individual element for a supply chain member, and discuss a method for assessing risk that considers only these individual elements. Earlier research has proposed methods for computing risk-related scores for suppliers, carriers and ports using benchmarks in the security arena [9-11]. We extend these methods here to consider both operational and disruptive risks throughout a supply chain.

One type of risk that has received a great deal of attention in the research literature is security related risk in the supply chain. These types of risks are especially difficult to assess, as a frequency-based approach is generally not viable. Security related practices at an organization may, however, be observed and compared to industry best practice as a way to determine how much risk is introduced by a particular supply chain member. This scheme may be operationalized by scoring an organization based on the degree to which these best practices are followed, using the International Ship and Port Facility Security (ISPS) code [11, 12]; the Supply Chain Security Orientation (SCSO) [13]; or industry-based best practices [9, 10, 14]. Closs and MacGarrell [10] and Bichou [11] provide a system of best practices for use in computing scores. For example, a carrier that has poor hiring practices poses a greater security risk to their operation than a carrier that performs both pre-hiring and post-employment background checks on its employees Similarly, a supplier that hasn't thought through the impact of key suppliers on their operation poses a greater risk than a supplier that has

identified alternative material sources in the case of a supply chain disruption.

Meixell and Norbis [9] develop a methodology for computing an overall assurance score in the security risk context, based on achievement of a minimally acceptable performance level for each indicator in thematic areas, for each supply chain member. The term "assurance" is used here to reflect the confidence one would have in an organization that adopts good practices in risk management. In security, for example, suppliers may be evaluated based on their observance of best practices in each of three themes: relationships, security efforts, and incident security management. Similarly, suppliers may be evaluated based on their likelihood in other categories as well, including those related to demand and supply uncertainties. This same approach is also readily applicable to other supply chain members including carriers and ports. Here, the individual risk score is calculated following the conventional approach that defines risk as the chance in quantifiable terms of an adverse occurrence [15] for each type as:

Risk Score Type I = 1-Assurance Score Type I [1]

Risk Score Type II = 1-Assurance Score Type II [2]

Individual risks may then be defined as:

sr_i Individual Type I risk for supplier i
$s\rho_i$ Individual Type II risk for supplier i
cr_j Individual Type I risk for carrier j
$c\rho_j$ Individual Type II risk for carrier j
pr_k Individual Type I risk for port k
$p\rho_k$ Individual Type II risk for port k

They are summarized in Table 1.

Table 1 Parameters for individual risk

	Suppliers	Carriers	Ports
Type I risk	sr_i	cr_j	pr_k
Type II risk	$s\rho_i$	$c\rho_i$	$p\rho_k$

As an example, consider a hypothetical case comparing the risk associated with 2 suppliers, 2 carriers and 2 ports. For these six possible supply chain members, individual assurance scores may be evaluated and individual risk scores calculated according to [1] and [2]. They are:

$sr_1 = .2$ $sr_2 = .1$
$s\rho_1 = .0001$ $s\rho_2 = .01$

$cr_1 = .1$ $cr_2 = .2$
$c\rho_1 = .02$ $c\rho_2 = .002$

$pr_1 = .5$ $pr_2 = .2$
$p\rho_1 = .001$ $p\rho_2 = .02$

These individual values may then be used as such to evaluate the risk that an individual member presents in a supply chain, perhaps useful in the supplier selection or development process. Their scores may also be combined to evaluate risks due to direct interactions and supply chain design, as we describe in the following sections.

Supply Chain Direct Interactions

Another influence on supply chain risk is the interaction effect between individual risk elements, as risk levels associated with individual supply chain members may be modified through supply chain relationships and their interactions. The risk score may be altered when information is shared between members, or when decisions are integrated to improve overall supply chain performance. For example, assurance may be improved when supply chain members collaborate [13, 16, 17] by sharing timely and valid information, by using RFID for tracking purposes, and by maintaining a high level of security in their own information systems [14].

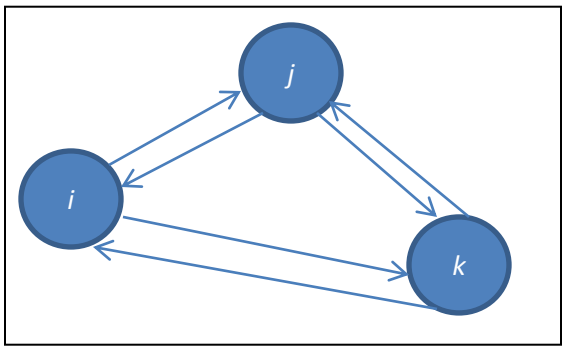
In this paper, we allow for this type of collaborative improvement to be factored into risk assessment, and call it direct interaction to differentiate it from the general interaction to which every member of the supply chain is subject to. We then develop rules to combine risk when one or more supply chain members interact directly. Finally, we propose a methodology to quantify the combined risk score, and illustrate it with a small case.

As partners of the supply chain communicate in an exchange of material, information and money, risk is passed along in the exchange in such a way that the risk of the combined members, in general, differs from the individual contributions to risk. In the proposed model, each member of the supply chain is characterized for each risk type by a risk score in the 0-1 scale where 0 represents a risk-free state and 1 represents the highest risk.

Following Wagner and Neshat [18], we propose a graphical model to represent these relationships and interactions. In this graphical model each member of the supply chain is represented by a node, and the connections between members are represented by directed arcs which represent in the authors' view, the main direction of the flow of risk. The graph in Figure 1 is such a schematic representation of a simple supply chain including three members, i, j and k. Supply chain members are represented by nodes and, as they interact, the risk that is passed through the interaction is represented by the directed arcs. For example risk of late deliveries and poor quality product flows in the same direction that the product does, while risk of wrong information may flow in both directions along the whole supply chain. On the

other hand Type II risk of disruption affects every member in the supply chain in contact with the product or the information. To evaluate the combined risk score for the unit constituted by two or more members in the supply chain we propose to combine the individual risk and the level of interaction under three rules.

Figure 1 Graphical representation of supply chain members and their risk interactions.



The first rule is *neutral interaction*. When the interaction between members in a supply has no effect on assurance, the risk factor for the combined unit equals the rating of the member with the highest risk factor. In other words, the weakest member drives the supply chain risk.

The second rule applies when there is *positive interaction* between the members in the supply chain. Here, interaction improves the assurance associated with the riskiest member. If one supply chain member is associated with another member with higher assurance due to better practices, then the overall risk for the unit equals the score for the member with the lowest risk.

The third applies when there is *negative interaction* between the members in the supply chain. Even if uncommon, it can be thought of a situation in which the interaction of two members would increase the overall risk of the supply chain beyond that posed individually by each member. In this case the highest risk will be multiply by a factor greater than 1. This could be the case, for example, of a carrier visiting a port of another nation in the proximity of war with the carrier's country of origin.

These interactive risks will be represented by r_{ijk} and ρ_{ijk} where:

r_{ijk} : Type I risk incurred by the direct interaction of member *i* with members *j* and *k*.

ρ_{ijk} : Type II risk incurred by the direct interaction of member *i* with members *j* and *k*.

The risk scores are calculated as functions of the individual risks which are derived from the previous rules and will be generically represented as:

$$r_{ijk} = f\ (sr_i, cr_j, pr_k)$$

$$\rho_{ijk} = \varphi\ (s\rho_i, c\rho_j, p\rho_k)$$

Following with the example, let's assume that because supplier 2 developed a partnership with carrier 2 and both operate out of port 2, then the r_{222} and ρ_{222} becomes the lower of the 3 risks in each type

$$r_{222} = \min\ \{ sr_2, cr_2, pr_2\} = \min\ \{.1, .2, .2\}=.1$$

$$\rho_{222} = \min\{s\rho_2, c\rho_2, p\rho_2\} = \min\ \{0.01, 0.002,0.02\}= 0.002$$

Now if we assume that between supplier 1, carrier 1 and port 1 there is no interaction that affects their operational or disruption assurance, the first rule of neutral interaction applies and the unit risk equals the highest risk of its members:

$$r_{111} = \max\ \{ sr_1, cr_1, pr_1\} = \max\ \{.2, .1, .5\}=.5$$

$$\rho_{111} = \max\{s\rho_1, c\rho_1, p\rho_1\} = \max\ \{0.0001, 0.02,0.001\}= 0\ .02$$

Supply Chain Structural Design

It is common practice in supply chain management to use supply chain structure to reduce risk. This is an example of using the structure of the supply chain to reduce risk. In this section, we generalize this practice to consider a variety of sub-structures, and then propose a method for incorporating structure in risk assessment.

It is possible to duplicate any of the elements in the supply chain, for example dual sourcing (applies equally to dual carrier or dual port) and it can be duplicated either in series as in parallel. The Type I risk for elements in series follows the addition rule of probability [19]. The Type II risk for elements in series is calculated as the maximum of the individual risks because it is assumed that as the disruption occurs, it stops all processes in the supply chain [20].

For elements in parallel, for the Type I risk, the multiplication rule of probability for independent events applies [19]. While for Type II risk, again it is assumed that when the disruption occurs it stops all processes and so the risk will equal the maximum of the risks.

Table 2. Type I and Type II risk for dual members in series and in parallel

	Series	Parallel
Type I risk	$sr_1 + sr_2 - sr_1 * sr_2$ (3)	$sr_1 * sr_2$ (4)
Type II risk	$max\ (s\rho_1\ ,\ s\rho_2)$ (5)	$max\ (s\rho_1\ ,\ s\rho_2)$ (6)

The previous argument applies equally to carriers and ports. The corresponding equations can be equally derivate.

Another structural situation is associated with the carrier's route. When a given carrier makes stops at multiple ports the risks associated with these ports are passed on to the carrier and they are modeled as described here. We assume that:

1. The cargo proceeding from original supplier is not altered at the new carrier stop.
2. No new cargo for this demand is loaded at any of these stops, because to do so will constitute multiple suppliers which is addressed in a separate part of this section.

Under these assumptions, the original cargo is subject to the risk of delays (Type I) associated with additional port(s) as well as with additional supplier(s) that even when not supplying our demand they incur in delays in the route. They are also subject to the risk of disruption because of catastrophic events associated with additional suppliers, ports or routes (Type II). It seems intuitive that the addition of elements in the supply chain would not decrease Type II risk. The risk involved in these situations was previously addressed in equations 3, 4, 5 and 6 as multiple suppliers and multiple ports in series.

Continuing with the example we are considering the two available suppliers for a dual sourcing in series and in parallel. The Type I and Type II risks scores are calculated following equations in Table 2 and the results are shown in Table 3.

Table 3. Type I and Type II risk for dual members in series and in parallel, example.

Supplier	Series	Parallel
Type I risk	.2 + .1 - .02= .28	.2*.1=.02
Type II risk	.01	.01

CONCLUSIONS AND NEXT STEPS

In this research, we present a framework to address the comprehensive nature of risk in the supply chain. In particular two different settings that influence the analysis of risk have been recognized and analyzed. The first consists in the separation of operational risk from disruption risk The other situation consist in the separation of individual risk inherently associated with an element independent of its relationships and the supply chain risk as a product of the interactions of element in the supply chain as well as the supply chain structural design.

An observation can be drawn from this analysis, that the duplication of sources (same as that of carriers or ports) recognized by some authors [20] [21] [22] as a method to minimize risk, actually minimizes operational risk but may increase disruption risks. The more members in a chain the more opportunities for disruption to occur and perhaps the less resilient the supply chain becomes.

The next step in this research effort should consist in the formulation of a mathematical model that incorporating these measures of risk will make design recommendations to minimize risk in the supply chain.

REFERENCES

[1] C. S. Tang, "Perspectives in supply chain risk management," *International Journal of Production Economics,* vol. 103, pp. 451-488, 2006.

[2] S. Chopra and M. S. Sodhi, "Managing risk to avoid supply-chain breakdowns," *Sloan Management Review,* vol. 46 pp. 53-61, 2004.

[3] P. R. Kleindorfer and G. H. Saad, "Managing disruption risks in supply chains," *Production and Operations Management,* vol. 14, pp. 53-68, 2005.

[4] G. A. Zsidisin, L. M. Ellram, J. R. Carter, and J. L. Cavinato, "An analysis of supply risk assessment techniques," *International Journal of Physical Distribution & Logistics Management,* vol. 34, pp. 397-413, 2004.

[5] S. Rao and T. J. Goldsby, "Supply chain risks: a review and typology," *International Journal of Logistics Management,* vol. 20, pp. 97-123, 2009.

[6] B. Richie and C. Brindley, "Supply chain risk management and performance," *International Journal of Operations and Production Management,* vol. 27, pp. 303-322, 2007.

[7] J. Gould, C. Macharis, and H. Haasis, "Emergence of security in supply chain management literature," *Journal of Transportation Security,* vol. 3, p. 287, 2010.

[8] Z. Williams, J. E. Lueg, and S. A. LeMay, "Supply chain security: an overview and research agenda," *International Journal of Logistics Management,* vol. 19, pp. 254-281, 2008.

[9] M. J. Meixell and M. Norbis, "Integrating Carrier Selection with Supplier Selection Decisions to Improve Supply Chain Security," *International Transactions in Operational Research,* vol. forthcoming, 2011.

[10] D. J. Closs and E. F. McGarrell, "Enhancing Security Throughout the Supply Chain," IBM

Center for the Business of Government, Washington, DC 2004.
[11] K. Bichou, "The ISPS Code and The Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management," *Maritime Economics & Logistics*, vol. 6, p. 322, 2004.
[12] International Maritime Organization, "International Ship and Port Facility Security (ISPS) code ". vol. 2011, 2004.
[13] C. W. Autry and L. M. Bobbitt, "Supply chain security orientation: conceptual development and a proposed framework," *International Journal of Logistics Management*, vol. 19, pp. 42-64, 2008.
[14] M. Voss, J. Whipple, and D. Closs, "The Role of Strategic Security: Internal and External Security Measures with Security Performance Implications," *Transportation Journal*, vol. 48, p. 5, 2009.
[15] K. Bichou and A. Evans, "Maritime Security and Regulatory Risk-Based Models: Review and Critical Analysis," K. Bichou, M. Bell, and A. Ewans, Eds., 2008.
[16] Y. Sheffi, "Supply chain management under the threat of international terrorism," *International Journal of Logistics Management* vol. 12, pp. 1-11, 2001.
[17] D. M. Russell and J. P. Saldanha, "Five tenets of security-aware logistics and supply chain operation," *Transportation Journal*, vol. 42, pp. 44-54, 2003.
[18] S. M. Wagner and N. Neshat, "Assessing the vulnerability of supply chains using graph theory," *International Journal of Production Economics*, vol. 126, pp. 121-129, 2010.
[19] G. Keller, *Statistics for Management and Economics*, 7th ed.: Thomson, 2005.
[20] M. Norbis and M. Meixell, "Dual Sourcing in the Supply Chain Design: A Multi-Dimensional Framework of Risk," in *IMSCI* Orlando, 2011.