Towards a formulation of a comprehensive risk model for an integrated supply chain: The use of graphical models to access structural risks.

Mario NORBIS
MANAGEMENT DEPARTMENT. QUINNIPIAC UNIVERSITY
Hamden, CT 06518 USA

and

Laoucine KERBACHE
HEC-Paris
78351 Jouy en Josas Cedex FRANCE

8th International Multi-Conference on Society, Cybernetics, and Informatics (IMSCI)
Orlando, FL. July 15-18, 2014.

ABSTRACT

Increasing economic uncertainty, demand instability, and supply interruption from natural 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. Moving towards the formulation of a comprehensive risk model, in this research, we develop a graphical approach to represent the risks generated by the supply chain structural design.

Keywords: Supply Chain Security, Risk Analysis, Supply Chain Management, Graphical Models.

INTRODUCTION

Managers struggle regularly with risk events that affect the performance of the supply chain. These risk events can be routine as late or short shipments from a supplier; or major disruptions as in the case of devastating earthquakes that interrupt supply for months or even years.

The precepts of risk management are especially pertinent in this context. Risk management process entails risk identification where a list of possible risk events is identified, followed by risk assessment and analysis where the impact and likelihood of each event is quantified. These steps are followed by risk response, 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 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.

Risk in any organization can be viewed as two-dimensional, i.e. the likelihood of the event occurring, and the impact or consequence on the organization if it does occur. [1]. Likelihood of any event is usually quantified as the probability, subjectively assigned or objectively calculated, of the event happening. In the case of risk, as it is generated by uncertainty it cannot be directly quantified [2][3] or the assessment of probability is so subjective that it turns the information useless [4]. In this context Meixell and Norbis [4] developed a framework based on Closs and McGarrell [5] to individually evaluate security scores for any member of the supply chain based on their practices in selected security related themes.

Tang [6] 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 [7] 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 [7] 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. Also for Wagner [8], characteristics of the supply chain are antecedents of supply chain vulnerability : occurrence and severity of disruption.

Thus, we consider two types of risk in this research: operational risk (Type I) and disruption risk (Type II).

A seminal article by Tang [6] 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 [7] on a framework that includes information systems and IP risks, and Kleindorfer and Saad [9] on disruption risks. Literature reviews on supply chain risk management include Zsidisin, Ellram, Carter and Cavinato [10]; Rao and Goldsby [11]; and Ritchie and Brindley [12]. There is also a great deal of literature concerning the focused topic of security, nicely summarized in Gould , Macharis and Haasis [13]; and Williams, Lueg and LeMay [14].

It has been proposed Meixell and Norbis (4) 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 to which individual members of a supply chain (e.g. suppliers, carriers, ports) are exposed. There are numerous elemental, individual risks in a typical supply chain; Closs and McGarrell discuss these elements at some length [5].

The second constituent on supply chain risk 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 to the supply chain will also affect the individual components of risk either increasing or decreasing them depending on the circumstances. This is also known as the network effect. 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, structural effects in this way can influence both Type I and Type II risks.

Within this framework, we define the research question guiding this effort as follows: how can we represent and measure the influences that supply chain structure has on the overall risk of the supply chain.

In this respect, graphical models has been frequently used for the evaluation of risk in the supply chain.

Wagner [8] quantifies vulnerability index using graph theory and also evaluates how propagation of vulnerability from one stage to other stages.

Bayesian networks has been more recently used by Lockamay III [3] Lockamay McCormack [15] and Shin [16] In Bayesian networks, a subjective believe of occurrence of hypothesis based on past experience is used to calculate the probability of the evidence provided that the hypothesis is true.

Lockamay III [3] used it to evaluate supplier risk impacts on buyers organization. A supplier risk profile score is created based in characteristics and relationship factors, past performance, disaster history and it is used to translate into risk probability. Lockamay McCormack [15] developed a methodology to modeling and then evaluate risk profiles in supply chains. Shin [16] relates supply chain risk and network structure. Transportation risk propagation is analyzed through Bayesian networks analysis to optimize transportation route concluding that risks are not independent and they have impact beyond directly connected vertex / nodes.

The propagation of risk through the network is also directly addressed by Huang [1], highly interconnected networks make possible propagation where risk cascade even with out attacks physically spreading through the network. Also Cheng [17] analyzes risk in different network structures and direct propagation to adjacent vertex / supply chain members. Also Wagner [8] vulnerability at one stage influences other stages vulnerability.

Shin [16] and Nagurney [18] develop network optimization models to address supply chain risk. Shin [16] uses Bayesian Networks to optimize transportation route and minimize risk propagation, concluding that risks are not independent and they have impact beyond directly connected vertex / nodes. Nagurney [18] develops a supply chain network model to optimize the decision-making in a multicriteria situation involving profit maximization and demand side risk minimization.

MODEL CONSTRUCTS

In this context our research follows Wagner and Neshat [8], in proposing a graphical model to represent the risk relationships and interactions in a supply chain and evaluate the structural component of risk.

Taking from Norbis and Meixell [19] we represent individual risk scores 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

Also following Norbis and Meixell [19] direct interaction risk scores, are calculated based on the individual risks and three rules of interaction, namely *Neutral interaction, positive interaction and negative interaction*

The first rule is *neutral interaction*. When the interaction between members in a supply has no effect on security, 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 security associated with the riskiest member. If one supply chain member is associated with another member with lower risk 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 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:

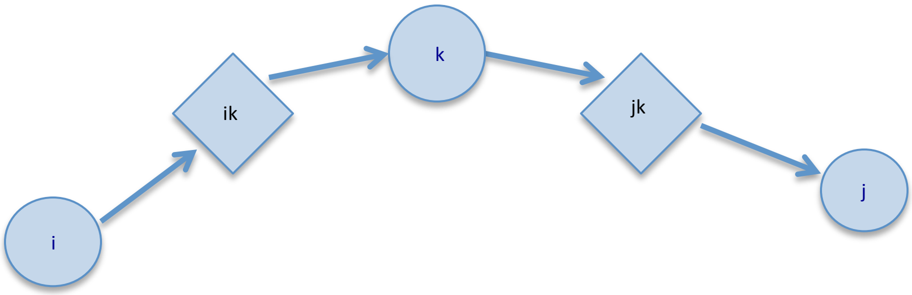
$$r_{ijk} = f\ (sr_i, cr_j, pr_k)$$

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

Norbis and Meixell [19]

In this graphical model a node represents each member of the supply chain, and the connections between members are also represented by nodes. Each of these nodes carries a value representing their contribution to risk. The graph in Figure 1 is a schematic representation of a simple supply chain including three members, i, j and k. Supply chain members are represented by round nodes and, as they interact, the risk that is passed through the direct interaction is represented by square nodes

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



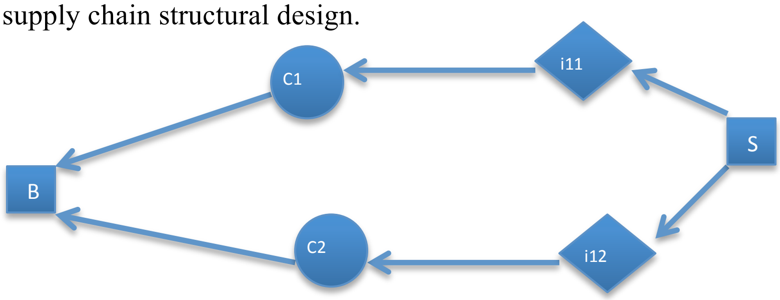
Our approach does not include a Bayesian network methodology as we minimize risk scores rather than dealing with subjectively assessed probabilities. We address risk propagation in two ways, through the evaluation of risk propagated by direct interaction of any 2 elements and through the influence of the supply chain structure on the overall risk. We sought to select a path among supply chain members to satisfy demand requirements while minimizing the overall risk score of the supply chain, optimizing the decision making as in Shin [16] and Nagurney [18]

We exemplify our approach with three different cases, one of direct interaction and 2 related to the supply chain structural design.

In each case we post the same question, in relative terms what would be the alternative that minimizes the overall risk from source(s) to destination. Methods are thought to evaluate the combine risk score.

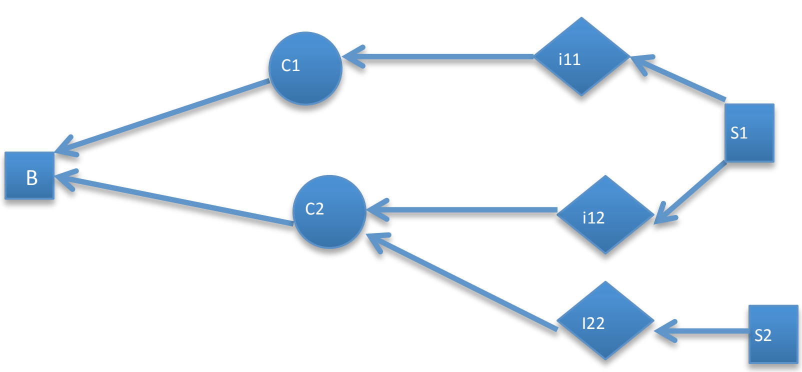
Case I. Interaction

Given a supplier S1 and carriers C1 and C2 with known individual risks:
Of type I, sr_1, cr_1, cr_2 and
Type II $s\rho_1$, $c\rho_1$, $c\rho_2$,
and with interactions risks of both type I and II
r_{11}, r_{12}
ρ_{11}, ρ_{12},



Which route will minimize the combine risk scores from source S1 to buyer B?

Case II. Structural
Case II-1 Routing



Given a suppliers S1 and S2 along with carriers C1 and C2 with known individual risks:

Of type I, sr_1, sr_2, cr_1, cr_2 and
Type II $s\rho_1$, $s\rho_2$, $c\rho_2$, $c\rho_2$,

and with interactions risks of both type I and II

r_{11}, r_{12}, r_{22}
ρ_{11}, ρ_{12}, ρ_{22}

we can further assume that C_1 and C_2 are identical carriers with identical individual risks and identical interaction risks, such that

$cr_1 = cr_2$
$c\rho_2 = c\rho_2$

and

$r_{11} = r_{12}$
$\rho_{11} = \rho_{12}$

Assume now that our only supplier is S1, but carrier C2 "touches" supplier S2 to pick-u (or deliver) merchandise for other customer.

How will this routing affect the overall risk? Which would be the combine risk score?

Case II-2 Doubling

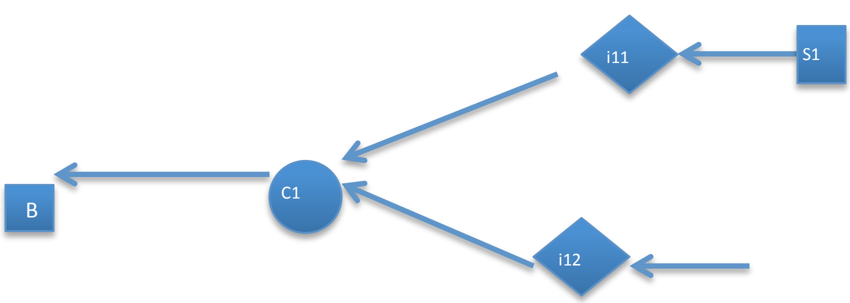
Here we compare doubling one member (say sources) both acting *simultaneously,* at the same time, versus sole source and then *alternate*, either one or the other at a time versus sole source.
Given a suppliers S1 and S2 along with carriers C1 with known individual risks:

Of type I, sr_1, sr_2, cr_1 and
Type II $s\rho_1$, $s\rho_2$, $c\rho_2$,

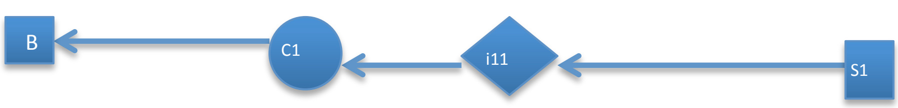
and with interactions risks of both type I and II

r_{11}, r_{12}, r_{22}
ρ_{11}, ρ_{12}, ρ_{22}

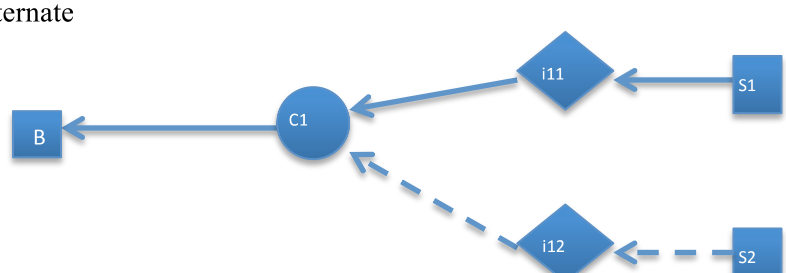
Simultaneous



Sole



Alternate



CONCLUSIONS AND NEXT STEPS

In this research, we present a framework to address the structural risk in the supply chain. In particular an approach is developed that recognizing the individual components of risk as well as the risk associate with direct interactions and proposes a graphical setting for the analysis of the risk associated with the structural design of the supply chain. Two cases are proposed to analyze these effects; the first addresses the effects that the carriers' routing may post on the supply chain overall risk. The second case addresses the effect of doubling one of the supply chain members, in this case the source.

An observation seems be drawn from this analysis, that the duplication of sources (same as that of carriers or ports) recognized by some authors as method to minimize risk, actually minimizes operational risk but may increase disruption risks.

The next step in this research 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.D. Huang, R.S. Behara and Q. Hu, "Managing Risk Propagation in Extended Enterprise Networks," *IT Pro IEEE Computer Society,* pp. 14-19, July/August 2008.

[2] F. H. Knight, "Risk, Uncertainty and Profit," *Houghton Mifflin, Boston, MA.* 1921

[3] A. Lockamy III, "Benchmarking supplier risks using Bayesian networks," *Benchmarking: An International Journal,* vol. 18, No. 3, pp. 409-427, 2011.

[4] M. J. Meixell and M. Norbis, "Integrating Carrier Selection with Supplier Selection Decisions to Improve Supply Chain Security," *International Transactions in Operational Research,* vol. 19, No. 5, pp. 711-732, 2012.

[5] D. J. Closs and E. F. McGarrell, "Enhancing Security Throughout the Supply Chain," IBM Center for the Business of Government, Washington, DC 2004.

networks," *Journal of Enterprise Information Management,* vol. 22, No. 4, pp. 345-360, 2008.

[18] A. Nagurney, J. Cruz, J. Dong, D. Zhang. " Supply chain networks, electronic commerce, and supply side and demand side risk," *European*

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

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

[8] 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.

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

[10] 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.

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

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

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

[14] 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.

[15] A. Lockamy III, K. McCormack, "Modeling supplier risks using Bayesian networks," *Industrial Management &Data Systems,* vol. 212, No. 2, pp. 313-333, 2012.

[16] K. Shin, Y. Shin, J. Kwon, S. Kang, "Risk propagation based dynamic transportation route finding mechanism," *Industrial Management & Data Systems,* vol. 112, No. 1, pp. 102-124, 2012.

[17] S.K. Cheng, B.H. Kam, "A conceptual framework for analysing risk in supply *Journal of Operational Research,* vol. 164, pp. 120-142, 2005.

[19] M. Norbis and M. Meixell, "Dual Sourcing in the Supply Chain Design: A Multi-Dimensional Framework of Risk," in *IMSCI* Orlando, 2011.