Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

FMEA based Quantification Analysis of Outbound Supplier Risk and its Resilience

Karthick. M[1] and Manikandan .V[2]

[1] Thiagarajar College of Engineering, Madurai

Received: 13 December 2013 Accepted: 3 January 2014 Published: 15 January 2014

Abstract

Supply chain is the linkage of series of organizations with facilities, functions, and logistic activities that are involved in producing and also delivering a product or service. In the past, when firms manufactured in-house, they sourced locally and sold directly to customer. During that period, supply chain risk was less diffused and easier to manage. In recent years global supply chain was hit by increasing globalization, because all organizations had to face vulnerable by different types of risk in their inbound and outbound supply chain network. The various supply chain (SC) vulnerabilities are reputation, unreliability, overstocking, price increases, corruption, natural disasters and financial failure. The implications of supply chain possessing vulnerability costlier and lead to significant customer delivery delays, etc. Though, different types of supply chain vulnerability management methodologies have been proposed for managing supply risk. To the above concern, reinforce outbound supply chain risk management by proposing an integrated methodology to classify, manage and assess outbound supply risks were made. The contributions of the work owing to namely (1) outbound supply risk factors are identified through both supply chain risk literature review and industrial interview; (2) Hierarchical risk factor classification structure is created; (3) reduction of outbound supplier risk by using six sigma methodologies was validated. This project is an attempt to quantify the outbound supplier risk with a suitable case study.

Index terms— increasing globalization, vulnerabilities are reputation, unreliability, overstocking, price increases, corruption, natural disasters and financial fa

1 Introduction

upply chain resilience is defined as the system ability to approach its equilibrium state, after being disturbed by external or internal factors. This consideration is following aspects: Supply Chain flexibility, agility, velocity, visibility and redundancy (Creating resilient SCs: A Practical guide, 2003). Flexibility helps companies in correctly answering to markets variability, the agility as the company capability to quickly respond to unpredictable demand/supply markets changes, the velocity must be interpreted as time required for moving goods along the supply chain. The velocity is usually measured in terms of lead times; the visibility is the capability of the company to see all the information regarding the flow of products, information and finances both downstream and upstream along the supply chain.

The redundancy is the augmentation of capacity and inventory in each node of the supply chain for facing supply chain disruption events (Christopher and ??utherford, 2004). This paper focused on outbound supplier risk in supply chain. Managing outbound supplier risk can be a challenging task due in part to the complex and dynamic nature of supply chain systems.A typical supply chain system can be large in scale, having many tiers of suppliers, where each supplier tier of the supply chain provides goods or services to the next level supplier tier in the supply chain. They are facing much risk in internal and external to the supply chain.

Supply chains expand globally; their risk of disruption also grows. Supply chain risk is a particular type of hazards or threats affect the supply chain performance. Commonly there are two types of risk in the supply chain. There are internal risk (quality, accident, fire, security, IT, marketing, building, human, etc.,) and external risk (political, economical, social, technological, environmental, terrorist attack, war, etc.). (Understanding Supply Chain Risk: A self assessment workbook, 2003).

2 II.

3 Literature Review

Christopher S. Tang (2006) reviewed various quantitative models for managing supply chain risks. We found that these quantitative models are designed for managing operational risks primarily, not disruption risks. However, we argue that some of these strategies have been adopted by practitioners because these strategies can make a supply chain become more efficient in terms of handling operational risks and more resilient in terms of managing disruption risks.

David Bogataj (2007) et.al suggested that the costs of risk in a supply chain, which is exposed to internal and external risk, are measured using net present value of activities approach. their consider financial risk (where the financial flow has the opposite direction to the flow of goods) increases with the extension of the network, especially when in globalization processes even the currency exchange rate in this flow is not always stable.

David J.Closs (2011) et.al developed a framework to examine the threat of potential disruptions on supply chain processes and focuses on potential mitigation and supply chain design strategies that can be implemented to mitigate this risk. There are focused with unintentional causes such as accidents or natural disasters, Intentional disruptions may include theft, illustrate that the depth and breadth of security initiatives depends on top management mindfulness, operational complexity, and product risk.

Hansuk Sohn (2011) et.al analyzed distributors' selection is based on the rough set theory approach in both equal and unequal weight features. Through this method, several rules are generated for distributors' evaluation and selection. The result not only shows the effectiveness of unequal weight incorporated rules identification, but also it shows the importance of the relationship intensity, marketing experience, and the management ability in selecting the distributors.

Jukkahalikas Sameer Kumar (2005) et.al proposed model is flexible and scalable and can be extrapolated for analysis of different nodes and layers in the existing disaster relief supply chains. This frame work was used in the example of the March 2011 disaster in Japan which was the result of a Tsunami, after a strong earth quake, followed by flooding and nuclear reactors' meltdown causing radiation dispersal. The failure mode effects and critical analysis method was used assess the reliability of a relief supply chain system and its critical components.

Sri Krishna Kumar (2013) et.al considered the location, production-distribution and inventory system design model for supply chain for determining facility locations and their capacity. Risk pooling effect, for both safety stock and running inventory (RI), have been incorporated in the system to minimize the supply chain cost along with determining facility location and capacity.

Stephen M.Wagner (2010) et.al developed an approach based on graph theory to quantify and hence mitigate supply chain vulnerability. their consider natural disasters such as droughts, floods, windstorms, hurrycanes, earth quakes or tsunamis strike more often and have a greater economic impact. At the same time, the number of man-made disasters such as accidents, wars, terrorist attacks, strikes, that affect supply chains.

Teresa Wu (2006) et.al considers the inbound supply chain risk management by proposing an integrated methodology to classify, manage and assess inbound supply risks. The contributions of this paper are four-fold: (1) inbound supply risk factors are identified through both an extensive academic literature review on supply risk literature review as well as a series of industry interviews; (2) from these factors, a hierarchical risk factor classification structure is created; (3) an analytical hierarchy processing (AHP) method with enhanced consistency to rank risk factor for suppliers is created; and (4) a prototype computer implementation system is developed and tested on an industry. Timothy J. Pettit (2008) consider the current thought on supply chain resilience and Develop the construct into a managerial process for implementation. Academics and industry leaders have seen the need to supplement traditional risk management techniques with the concept of resilience that is better designed to cope with extreme complexities, unpredictable events and adaptive threats.

J.Vander Vorst (2002) et.al considers the factors are Changes in markets, products, technology, competitors and Governmental regulations.

Walter Zinn (2009) et.al proposed process builds upon an existing risk analysis framework by incorporating an innovative methodology used by the insurance industry to quantify the risk of multiple types of catastrophic events on key supply chain locations. Supply chains are increasingly vulnerable to catastrophic events such as hurricanes or terrorist attacks III.

4 Resilience Framework

Supply chain resilience is defined as the system ability to approach its equilibrium state, after being disturbed by external or internal factors. The main objective of the supply chain management is minimizing the cost and maximizing the customer satisfaction. However, improving supply chain resilience requires an appreciation that supply chain vulnerabilities may come in many guises, and the drivers of risk operate at several different levels.

Flexibility helps companies in correctly answering to markets variability, the agility as the company capability to quickly respond to unpredictable demand/supply markets changes, the velocity must be interpreted as time required for moving goods along the supply chain.

The velocity is usually measured in terms of lead times; the visibility is the capability of the company to see all the information regarding the flow of products, information and finances both downstream and upstream along the supply chain. The redundancy is the augmentation of capacity and inventory in each node of the supply chain for facing supply chain disruption events (Christopher and Rutherford, 2004). Supply chains expand globally; their risk of disruption also grows. Supply chain risk is a particular type of hazards or threats affect the supply chain performance. Supply chain vulnerability can be defined as an exposure to serious disturbance, arising from risks within the supply chain well as risk external to the supply chain (Timothy Pettit, 2010).

IV.

5 Levels of Analysis of Resilience

The main objective of the supply chain management is minimizing the cost and maximizing the customer satisfaction. However, improving supply chain resilience requires an appreciation that supply chain vulnerabilities may come in many guises, and the drivers of risk operate at several different levels. The multi-level framework outlined above breaks-down the problem of supply chain vulnerability into its constituent parts, nevertheless it should be born in mind that when an event occurs it may impact at several levels, as the celebrated example of Nokia and Ericsson illustrates (see below). The Nokia/Ericsson example highlights the vulnerability of industries with capacity constrained production and also raises other important themes, such as the issue of common components and the consequential nature of supply chain risks. The latter is in turn linked to the fact that supply chains are linear processes within complex systems of interacting networks b) NOKIA and ERICSSON In March 2000 worldwide demand for mobile telephones was booming. Two of the international market leaders were Finnish electronics company Nokia and its Swedish rival Ericsson. This is the tale of how an 'Act of God' half a world away would set off a train of events that would eventually precipitate a major competitive re-alignment.

The story starts on the evening of March 17th 2000, with a thunderstorm over central New Mexico. A lightning bolt hit a power line, which caused a fluctuation in the power supply, which resulted in a fire in a local semiconductor plant owned by Dutch firm Phillips Electronics NV. The fire was brought under control in minutes, but a batch of trays containing enough silicon wafers for thousands of mobile phones were destroyed in the furnace. The damage to the factory from smoke and water was much more extensive than the fire itself, contaminating the entire stock of millions of chips. The suppliers immediately prioritized customers, according to the value of their business. Between them, Nokia and Ericsson accounted for 40% of the plant's output of the vital radio frequency chips, so these companies were put at the top of the supplier's list.

On 20th March, in Finland Nokia's event management systems indicated that something was amiss. Orders were not coming through as expected, so a components purchasing manager phoned the supplier who informed him that there had been a fire in the plant, which would disrupt production for around a week. Nokia was not unduly alarmed, but dispatched engineers to New Mexico to investigate the situation. Philips were not encouraging visitors, so having been unable to investigate the problem further, Nokia increased monitoring of in-coming supplies from weekly to daily checks. It became clear soon afterwards that the problem was so serious that supplies would be disrupted for months.

Pressure was brought to bear at the highest levels between Nokia and its supplier to ensure that all other Philips plants were commissioned to use any additional capacity to meet Nokia's requirement. In addition, Nokia immediately sent representatives out to its other suppliers in the US and Japan to secure priority status for all available supplies of chips, and persuaded them to ramp up production as quickly as possible.

Because Nokia was such an important customer, they obliged with a lead-time of less than one week.

Nokia also set about reconfiguring its products to take slightly different chips from other sources. Ericsson had also found out about the fire soon after it occurred, but having been by the suppliers that the fire was unlikely to cause a major problem, had not acted further until early April.

By then Nokia had already moved to secure its supplies, and unlike the quick acting Finns, Ericsson had no alternative sources of supply. Ericsson lost an estimated $400m in new product sales as a result of the fire. An insurance claim would later offset some of Ericsson's direct losses; nevertheless it was forced to cease manufacturing mobile phones.

V.

6 Details of the Six Sigma Tool

The DMAIC toolkit is without question the most effective process improvement framework known in industry today, and teams that learn and apply this methodology will achieve unprecedented success.

The five stages of DMAIC cycle, Failure Mode and Effect Analysis (FMEA) is a tool that makes it possible to determine a system's possible modes of risk, and then to establish the effects of those risks on the Overall performance of the system.

FMEA is widely used as a quality improvement tool that can be applied equally to physical systems (vehicles, aircraft, electronic devices and so forth) and non-physical systems such as supply chain processes. The purpose of

FMEA is to prevent process and product problems during the design phase. However, conducting an FMEA on existing processes is also hugely beneficial; unlike products, processes can be reengineered more easily. c) Using FMEA (or FMECA), businesses can

? Exhaustively identify and catalogue the various ways in which links and nodes in the supply chain may fail.

? Determine the effects of those risks.

? Rank risks according to their likelihood of occurrence, their disruptive effect and the likelihood that imminent risk can be detected in time to put in place remedial action. Combined, this then gives an estimate of criticality, in order to guide preventative action. Rate how severe this effect is with 1 being not severe at all and 10 being extremely severe. Ensure the team understands and agrees to the scale before you start. Also, make this ranking system "your own" and don't bother trying to copy it out of a book.

Identify the causes of the failure mode/effect and rank it as you did the effects in the occurrence column. This time, as the name implies, we are scoring how likely this cause will occur. So, 1 means it is highly unlikely to ever occur and 10 means we expect it to happen all the time. Identify the controls in place to detect the issue and rank its effectiveness in the detection column. Here a score of 1 would mean we have excellent controls and 10 would mean we have no controls or extremely weak controls. Multiply the severity, occurrence, and detection numbers and store this value in the RPN (risk priority number) column. More than one occurrence per day or a probability of more than three occurrences in 10 events. 9

High: Risk occurs almost as often as not.

One occurrence every three to four days or a probability of three occurrences in 10 events. 8

High: Repeated risk.

One occurrence per week or a probability of 5 occurrences in 100 events. 7

High: Risk occurs often.

One occurrence every month or one occurrence in 100 events. 6 Moderately High: Frequent risk.

One occurrence every three months or three occurrences in 1,000 events.

7 5

Moderate: Occasional risk.

One occurrence every six months to one year or five occurrences in 10,000 events.

8 Moderately

Low: Infrequent risk.

One occurrence per year or six occurrences in 100,000 events.

3 Low: relatively few risks.

One occurrence every one to three years or six occurrences in ten million events. 2

Low: Risks are few and far between.

One occurrence every three to five years or 2 occurrences in one billion events. 1

Remote: Risk is unlikely.

One occurrence in greater than five years or less than two occurrences in one billion events.

iii. Detection rating scale VI.

9 Results and Discussions

The various inbound and outbound risks are listed VII.

Prioritization of the Outbound Supplier Risk The highest RPN values in outbound supplier risks are market characteristics, political stability and demand flexuation. But the demand risk is already focused in many literatures and mitigated by using suitable forecasting techniques. So first we mainly focused on political and market characteristic risks. [1]

[1] © 2014 Global Journals Inc. (US)

31

Figure 1: Figure 3 . 1

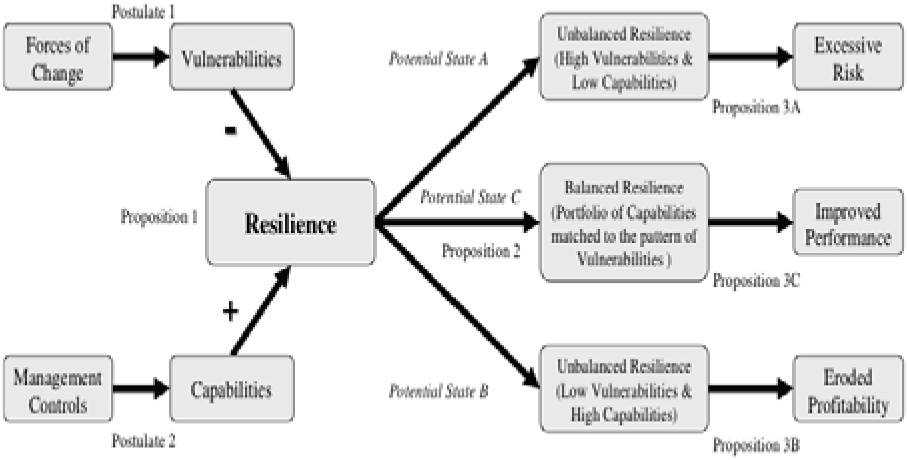
32 

Figure 2: Figure 3 . 2 a

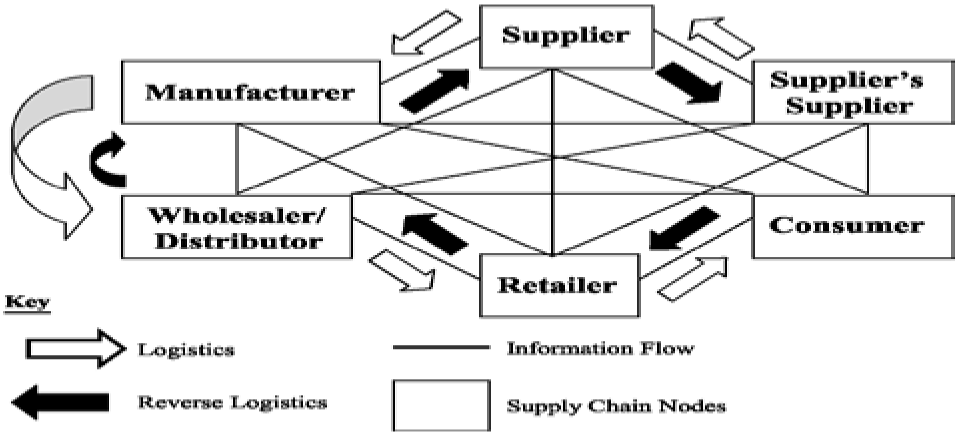


Figure 3: FMEA

5

1

Figure 4: Table 5 .

5

.5

Rating	Description	Definition
10	Absolute Uncertainty	Risk is not detectable and uncontrollable.
9	Very Remote	The risk can be detected only with thorough inspection and this is uncontrollable.
8	Remote	Risk is detected based on no effects in a events.
7	Very Low	The risk can be detected with manual inspection but no effects is in place so that detection is left to chance

Figure 5: Table 5

6

.1

[Note: © 2014 Global Journals Inc. (US)]

Figure 6: Table 6

7

	.1	
	Outbound supplier risk	
Priority number	Potential failure mode	RPN
1	Market characteristics	360
2	Political stability	350
3	Demand	336
4	External legal issues	252
5	Natural/man-made disaster	100
6	Security	80
7	II tier supplier	64

Figure 7: Table 7

.1 This page is intentionally left blank

[Int.J.Production economics] , *Int.J.Production economics* 119 p. .

[Int.J.Production economics] , *Int.J.Production economics* 90 p. .

[Int.J.logistic management] , *Int.J.logistic management* 23 p. .

[Computers Industrial Engineering] , *Computers & Industrial Engineering* 64 p. .

[Wagner and Neshat ()] , Stephan M Wagner , Nikrouz Neshat . 2010.

[Wu and Blackhurst ()] ‘A model for inbound supply risk analysis’. Teresa Wu , Jennifer Blackhurst . *Computers in Industry* 2006. 57 p. .

[Sohn et al. ()] ‘A rough set based approach to distributor selection in supply chain management’. Hansuk Sohn , Guofang Song , Rafael Gutierrez . *Expert Systems with Applications* 2011. 38 p. .

[Goh et al. ()] ‘A stochastic model for risk management in global supply chain networks’. Mark Goh , Y S Joseph , Lim . *European Journal of Operational Research* 2007. 182 p. .

[Assessing the vulnerability of supply chains using graph theory Int.J.ProductionEconomics] ‘Assessing the vulnerability of supply chains using graph theory’. *Int.J.ProductionEconomics* 126 p. .

[Kumar ()] ‘Before and after disaster strikes: A relief supply chain decision support framework’. Sameer Kumar , Thomashavey . *Int. J. Production Economics* 2005.

[Speier and Closs ()] ‘Global supply chain design consideration: Mitigation product safety and security risks’. Cheri Speier , David J Closs . *Journal of operation management* 2011. 29 p. .

[Nurmaya Musa and Tang ()] ‘Identifying risk issues and research advancement in supply chain risk management’. S Nurmaya Musa , Ou Tang . *Int.J.Production economics* 2011. 133 p. .

[Van Der et al. ()] ‘Identifying sources of uncertainty to generate Supply chain redesign strategies’. J Van Der , A Vorst , Beulens . *International Journal of Physical Distribution and Logistics Management* 2002. 33 p. .

[Bogataja and Bogataj ()] ‘Measuring the supply chain risk and vulnerability in frequency space’. David Bogataja , Marija Bogataj . *Int.J.Production Economics* 2007. 108 p. .

[Tang ()] ‘Perspectives in supply chain risk management’. Christopher S Tang . *Int. J. Production Economics* 2006. 103 p. .

[Zinn et al. ()] ‘Proactive planning for catastrophic events in supply chains’. Walter Zinn , Michael Knemeyer , Cuneyt Eroglu . *Journal of Operations Management* 2009. 27 p. .

[Jukka Hallikas and Urho Pulkkinen ()] *Risk management process in supplier network*, Jukka Hallikas , Urho Pulkkinen . 2004. (Iris karvonen)

[Chen and Cheng ()] ‘Supply chain management with lean production and RFID application: A case study’. James C Chen , Chen-Huan Cheng . *Expert systems with applications* 2013. 40 p. .

[Mccormack and Peter Trkman ()] *Supply chain risk in turbulent environment-A Conceptual model for managing supply chain network risk*, Kevin Mccormack , Peter Trkman . 2009.

[Samir Dani and Kalawsky ()] *Supply chain risk management: Present and future scope*, Roy Samir Dani , Kalawsky . 2012.

[Sri Krishna Kumar and Tiwari ()] *Supply chain system design integrated with risk pooling*, M K Sri Krishna Kumar , Tiwari . 2013.