

THE ROLE OF COMPETITIVE INTELLIGENCE LEVERAGE IN SUPPLY CHAIN RISK MANAGEMENT STRATEGY

Chris I. Enyinda

School of Business, Alabama A & M University

Charles Briggs & Won W. Koo

North Dakota State University

ABSTRACT

The desire for organizations to attain sustainable competitive advantage is moving SCRM issues up the corporate agenda. In current day operating environment, cost competitive advantages associated with outsourcing, alternative supplier base, lean supply chain, just-in-time supply chain, transferable technology, and acquisitions and mergers are rarely sustainable because they are easily replicated by competitors. As a result, the conduit to gaining sustainable competitive advantage may lie in supply chain competitive intelligence. By leveraging supply chain competitive intelligence within the context of the supply chain risk management strategy, organizations can build and maintain sustainable competitive edge. Since supply chain C-level executives are more than ever facing today's turbulent operating environment, a guide is needed to aid them in their quest for SCRM strategy. Because many things can and do get disrupted, SCRM is no longer an option, it has become a necessary requirement to thrive and survive. As a result, C-level executives are increasingly mandating adoption of SCRM strategy from their top supply chain leaders. This means they must understand portfolio of risks that may hinder gaining sustainable competitive advantage. Those organizations that lack the ability to properly manage their supply chain risks will run the risk of disrupting their materials and information flows which in turn can wreak havoc on near real-time responsiveness, loss of consumers' confidence, poor financial performance, and decrease in shareholders' value. The present paper proposes competitive intelligence approach to managing supply chain risks.

INTRODUCTION

While globalization, outsourcing, lean supply chain, supply chain quality management, and global just-in-time supply chain management initiatives have enhanced the ability of firms to contain costs, focus on their strategic core competencies, and improve operational efficiencies and effectiveness, the same initiatives have created an avalanche of risks thus making global supply chains more vulnerable, less resilient to disruptive risks (Enyinda et al, 2008), and increasingly susceptible to both high-impact and low-impact disruptive events (Sheffi and Rice, 2005). With the increasingly complex global business landscape that is the hallmark of ultra-competitiveness, supply chains are faced with alphabet soup of microeconomic and macroeconomics risks and uncertainties.

Holton (2004) described risk as composed of exposure and uncertainty. Adams (1995) posits that “virtually all the formal treatments of risk and uncertainty in game theory, operations research, economics and management science require that the odds be known, that numbers be attachable to the probabilities and magnitudes of possible outcomes.” Indeed, risk and uncertainty are the quintessential part and parcel of doing business. March and Shapira (1987) and Buehler and Pritsch (2003) contend that risk assumption is ultimately a fact of business and management life. Hence it is the ability to assume and manage risks is what organizations must do to produce profits and shareholder value (Buehler and Pritsch, 2003) and indeed “in extremely uncertain environments, shaping strategies may deliver higher returns, with lower risk, than they do in less uncertain times” (Courtney, 2001). Those organizations that hesitate to create order out of chaos (Courtney, 2001), manage risks and improve their risk management processes will be faced with a different kind of risks, including unexpected and severe financial losses that make their cash flows and stock prices volatile and harm their reputation with customers, employees, and investors (Buehler and Pritsch, 2003) and higher risk of system failure.

Supply chain risk pertains to any threat of interruption to the well functioning of supply chain operations (Christopher, 2003). Risk emanate from lack of knowledge about the nature of events that may disrupt supply chain operations and its resiliency to disruption (Deleris and Erhum, 2005). Global supply chain risks can negatively affect the operational and financial performance of firms. Hendricks and Singhal (2003) reported that when firms announced a delay to promised deliveries due to supply chain glitches led to a decline in shareholder value by 10.28%. Also, Hendricks and Singhal’s (2005) study of 800 firms that announced a supply chain disruption between 1989 and 2000 reported that during a three-year period, disrupted firms experienced a 33 to 40 per cent decline in stock returns relative to comparable industry counterparts. In the year leading up to firms broadcasting a supply chain disruption, they experienced a seven per cent reduction in sales growth, an 11 per cent increase in costs, and a 14 per cent increase in inventories. Knight and Pretty (1996) asserted shareholder value decreased by approximately 8% with a recovery time of 50 trading days as a result of supply chain disruptive risks. The Rice and Caniato (2003) reported that it cost a firm about \$50 million to \$100 million each day its supply chain was disrupted. Ericsson lost approximately \$400 million in sales because of the 2000 fire at a Philips microchip manufacturing plant in Albuquerque that disrupted supply of major components used in mobile phones (Eglin, 2003). To prevent future sudden disruptions, Ericsson implemented business continuity plans and new processes and tools (Norrman and Jansson, 2004).

To minimize the negative implications of disruptions prevalent in the present global economy, organizations must manage supply chain risks in order to gain sustainable competitive advantage. And gaining competitive advantage demands firms to adopt a set of robust supply chain risk management (SCRM) strategies that can deal with risks and uncertainties (Simchi-Levi et al, 2002, Christopher 2003). The concept of SCRM is still in its embryonic stage, and its understanding is limited, both in terms of key issues and implementation. As a result, “...while faced with new challenges of what appears to be an increasingly “uncertain” [operating] environment, practitioners [as well as C-level supply chain executives] have little guidance on their SCRM” (Jutter *et al.*, 2003). In view of this and in an era of unprecedented ultra-

competition, organizations of all measure must leverage competitive intelligence (CI) capability to create the actionable intelligence needed to reduce risks and uncertainties facing today's global supply chains. Thus, organizations can no longer afford to continue in their archaic "gut feeling" business approach as opposed to leveraging innovative strategies such as CI that can deliver real-time granular actionable intelligence needed to proactively manage global supply chain risk, create effective business strategies, buttress positional advantage, and substantially improve revenue streams. Therefore, the new agenda calls for organizations to leverage the CI as a competitive weapon to gain edge over rivals.

The paper reviews SCRM relevant literature and discusses the relevance of CI in the context of competitive advantage. Specifically, the paper proposes leveraging CI in SCRM strategy and how it can be used as SCRM strategy to deliver actionable intelligence for forward looking organizations. CI can be the crucial difference between succeeding and failing. CI-based SCRM can be beneficial to organizations in several ways, including having fewer surprises, making better and real-time decisions, attaining a better balance between opportunities and threats, gaining competitive and positional advantage, ability to anticipate and respond proactively to external trends and developments, focusing on uncertainties as opposed to certainties, and achieve greater influence over suppliers and managing them effectively (O'Brien and Joyce, 2007); Deloitte, 2004). Also, it can be a great differentiator for firms willing to build and enhance shareholder value.

REVIEW OF RELEVANT LITERATURE

Supply Chain Risk Management

Although supply chain management has been touted as a source of building sustainable, and gaining competitive edge (Hendricks and Singhal, 2003), improved financial performance, and shareholder value creation (Chopra and Meindl, 2001), firms can no longer guarantee the past achievements because of today's risks and uncertainties. However, in recent years, the relevance of risks and uncertainty in supply chain has received an avalanche of attention from academics, practitioners, (Hendricks and Singhal, 2005; Kleindorfer and Van Wassenhove, 2004; Cavinato, 2004; Kleindorfer and Saad, 2005; Towill, 2005; Peck, 2006; Barry, 2004; Christopher, 2003; Christopher and Lee, 2004; Zsidisin *et al.*, 2004; Spekman and Davis 2004; Enyinda, Tolliver, and Szmerekovsky, 2007), Wall-street, and governments. Regrettably, despite that supply chain risks have been receiving a great deal of attention and continue to rise, C-level executives have not done enough and are unprepared to implement SCRM. Although there is no one best way of defining SCRM, it represents the process of managing and mitigating risk through the application of risk management tools, collaboration and coordination among shareholders to enhance supply chain effectiveness and financial performance, and to reduce supply chain vulnerability as a whole (Tang, 2006; Norman and Jansson, 2004, Juttner *et al.*, 2003, Norman and Lindroth, 2002). Studies of uncertainty and risks and risks management have been examined in agricultural economics (Moschini and Hennessy, 1999); economics (Tversky and Kahnemann, 1992); finance (Smith *et al.*, 1990); management (Simons, 1999); and international business (Miller, 1992). SCRM is an emerging field that has garnered significant importance in recent years because of rising uncertainties and ever greater risks in

global supply chains. Therefore, to insure efficient and effective supply chain performance in the global business environment that is afflicted with uncertainty and risks associated with relenting threats of terrorism, natural disasters, pandemic, public policies, etc. requires proactive and effective risk management and full support of supply chain partners.

Kleindorfer (2000) argued that to mitigate risks in supply chain one must first identify the underlying sources of risks. By risk mitigation, Miller (1992) means those strategic actions firms must pursue to thwart risks or threats identified from wide range of sources. Therefore, because risks are caused by unexpected events and uncertainty, it is necessary to identify and categorize the sources of risks in global supply chains. Global supply chain risks can emanate from various forms. Due to the inherent complexities of the physical and economic systems, most risks cannot be forecast with absolute accuracy (Moschini and Hennessy, 1999). For supply chain context, sources of risks can be classified into three groups (Juttner *et al.*, 2003): (1) Environmental (external) risk sources include market risk (e.g., exposure to adverse market price movements such as value of securities, exchange rates, interest rates or spreads, and commodity prices); business-volume risk (e.g., changes in demand or supply from competition, exposure to revenue volatility); natural disaster; geopolitical action; public policies; among others. (2) Organizational (internal) risk sources include operational risks (e.g., exposure to loss due to inadequate internal processes and systems, labor strike or lack of skilled labor, machine breakdown). (3) Network-related risk sources within the supply chain are lack of ownership, chaos, and inertia (Christopher and Lee, 2001). Lack of ownership risk sources in supply chains can lead to little or no control because of ambiguous lines of responsibility; chaos risk sources are those linked to over-reactions, unwarranted interventions, false alarm, lack of transparency, etc.; and inertia risk sources emanate from the inability of organizations to sense and respond to changing environmental and market conditions (Juttner *et al.*, 2003).

Further, organizations' exposure to risk appeared to be increased by inter-organizational networking (Finch, 2004). Brindley and Ritchie (2004) classified the types of risks encountered in the supply chain into environment characteristics such as generic technologies, economic trade groupings, politics and national cultures can pose risk exposure for business organizations; industry characteristics are associated with changes within a specific industry that will pose risks for firms operating within or relating to the industry. These changes may be attributable to the industry's response to the wider environmental development due to changes in competitive strategies or reconfiguration of the supply chain structure and membership; and organizational characteristics are associated with reacting to changes in the competitive environment or actions to thwart anticipated risks. Van Landeghem and Vanmaele (2002) posit that sources of uncertainty in supply chain include customs regulations, price changes, information delays, competitor action, political environment, stochastic cost, available capacity, supplier quality, manufacturing yield, and internal organization. Hiles and Barnes (2001) classified sources of risks into five core groups, including strategic, financial, operational, commercial, and technical. Deloach (2000) points out that sources of risks can be grouped into three spheres, mainly the external risk emanating from competitors, customer needs, technological innovations, political, legal, regulatory, financial markets, and natural disasters; internal risk is related to operations, information processing, and financial issues related to price, liquidity, and credit; information risk is associated with incomplete, inaccurate, or obsolete information.

Given the long-term impact of supply chain disruption risks on organizations' market shares and public image, mitigating and managing risks and uncertainties have become unequivocally imperative. It is not only socially responsible and good business (Kleindorfer, 2000); it drives business value (Peleg-Gillai *et al.* 2006). According to Murphy (2006), "within publicly held US companies, Sarbanes-Oxley legislation has increased the level of executive responsibility for the accuracy of financial forecasts. Since supply chain performance impacts the accuracy of financial forecasts, executives have reason to acquire a deeper understanding of supply chain risks and early warning on events that can impact financial performance." For firms to optimize their financial performance, it "requires on going analyses of key risks spanning the entire supply network that connect suppliers, manufacturers, distributors, retailers, and customers. Analyzing the supply chains with the perspective of risks gives organizations a better understanding of the potential sources of a disruption, and, most importantly, the potential financial impact resulting from the disruption" (Lowery, 2004). However, in spite of these concerns and the ever growing mandate by Wall Street and shareholders for firms to engage in SCRM, a significant number of firms are not only complacent and oblivious to the havoc that supply chain risks can inflict on the balance sheets, assets, and revenue, but also the detriment to their reputations. For example, Mitroff and Alpaslan (2003) reported that only a mere 5% to 25% of Fortune 500 companies are girded to deal with disruptions and/or crisis.

Kleindorfer and Saad (2005) asserted that continuous coordination, cooperation, and coordination among supply chain partners are imperative for risk avoidance, reduction, management and mitigation such that the value and benefits created are maximized and shared fairly. From the preceding, one can conclude that to ensure a successful SCRM and in turn improve supply chain effectiveness and financial performance, coordination, collaboration, cooperation, application of risk managements, and of course information sharing, visibility and/or transparency are necessary ingredients. However, because of asymmetry of information some firms opportunistically manage and mitigate their individual risks without considering the total supply chain goals and objectives. Indeed, Harland *et al.* (2003) advocated that to manage and mitigate the propensity of supply chain risk exposures, it is necessary for firms to identify both individual risks as well as the potential risk sources at every link across the supply chain networks.

Kleindorfer and Van Wassenhove (2004) and Kleindorfer (2000) suggest that in order to manage and mitigate supply chain risks one must execute following integrated processes: (1) identifying underlying sources of risks, (2) determining the gateways by which such risks can manifest, (3) assessing the potential impact of these risks under various scenarios, and (4) providing the measures for mitigating and coping with these impacts. Based on their literature, Bandyopadhyay *et al.* (1999) reported that key components of risk management include (1) risk identification, (2) risk analysis, (3) risk reduction, transfer and acceptance, and (4) risk monitoring. Indeed, as many organizations continue to face growing disruption risks to their global supply chain logistics, they are under pressure to manage and mitigate these risks. However, Faisal *et al.* (2007) argued that understanding of the variables associated with risk mitigation and their relative interdependencies are the most difficult part of SCRM. Peck (2006) puts it that the primary goal of risk management is to identify and quantify the potential sources of risks, control and reduce specific narrowly defined risks.

From an agency theory context, risk determination methods can enable information gathering by firms to reduce inbound supply risks and uncertainty (Zsidisin *et al.*, 2004). Firms can successfully manage and mitigate risk when they understand the sources of risks and practice proactive management (Zsidisin *et al.*, 2004; Smeltzer and Siferd, 1998). Harland *et al.* (2003) suggest that the inherent risk in an organization's overall supply network can be managed and mitigated by identifying, evaluating, quantifying supply risk probability of occurrence, and exposure. Based on their review of literature, Faisal *et al.* (2006) reported that the selected factors that can affect SCRM are (1) information sharing, (2) agility in the supply chain, (3) trust among supply chain partners, (4) collaborative relationships among supply chain partners, (5) information security, (6) corporate social responsibility, (7) aligning incentives and revenue sharing policies in a supply chain, (8) strategic risk planning, (9) risk sharing in a supply chain, (10) knowledge about risks in a supply chain, and (11) continual risk analysis and assessment. For SCRM to be successful, Zsidisin *et al.* (2000) asserted that it requires continuous communication, gathering and analysis of relevant information that can enable development of appropriate risk management strategies. Similarly, Giunipero and Percy (2000) noted that development of risk management skills such as awareness of risk signals and risk management plans are important for supply risk management success. Kleindorfer and Van Wassenhove (2004) contend that supply chain design, contracting, and risk management systems are the approaches that global firms have typically used to deal with supply chain risks.

Christopher and Lee (2004) argued that one key factor in any strategy designed to manage and mitigate supply chain risk is to improve end-to-end information visibility which in turn can help to improve supply chain "confidence" for shareholders. Shareholders' confidence in supply chain can deteriorate if there is delay in material/product, information, and finance flows from one part of the supply chain to another. Visibility has long been recognized as vital to achieving supply chain efficiency and positional advantage. Thus, to have visibility, supply chain managers must have the knowledge associated with risks (threats) and opportunities through competitive intelligence. Indeed, the importance of visibility was recognized about 46 years ago when management guru, Drucker (1962) noted that "most of our present concepts focus on production or on the stream of money and credit, rather than on the flow of physical goods and its economic characteristics...To get control of distribution [risk], there requires seeing-and managing..." For example, Aberdeen Group (2006) reported that 79% of large organizations surveyed indicated that a lack of critical supply chain process visibility was their area of most concern. One of the ways to gain visibility and control is through access to timely information necessary to thwart supply chain risks. Also, Porter and Miller (1985) contend that new information flows can improve a firm's ability to exploit the internal and external linkages and in turn helps the firm to gain competitive advantage.

COMPETITIVE INTELLIGENCE

The field of CI has its root in military intelligence as documented in *The Art of War* by Sun Tzu (Griffith, 1976). In the 1990s, CI became an integral part of the "learning" organization (Prescott, 1999) for a significant number of organizations (Kahaner, 1996; Fuld, 1995; Goshal and Westney, 1991) because of the continuous change in global competitive landscape, quality management initiatives, and the view that actionable intelligence can be the key to achieving

sustainable competitive advantage (Prescott and Gibbons, 1993). Prescott (1999) described CI as an organizational process designed to develop actionable intelligence pertaining to competitive dynamics (e.g., moves and countermoves of competitors, suppliers, customers, alliance partners, and potential competitors), non-market factors (e.g., government regulation, tariffs, culture of a country), and to serve such important roles as early alert of opportunities and threats (risks), decision making support, competitor monitoring and assessment, and strategic planning support. Also, CI focuses on the various aspects of an organization's environment, including political, social, economic, technological, competitive, and ecological (Prescott, 1999). McGonagle Vella (2002) emphasized that the two important aspects of CI are mainly the utilization of legally and ethically sources to extract data on environmental conditions, competition, competitors, trends and scenarios; and the transformation of data into actionable information that can support real-time organizational decisions.

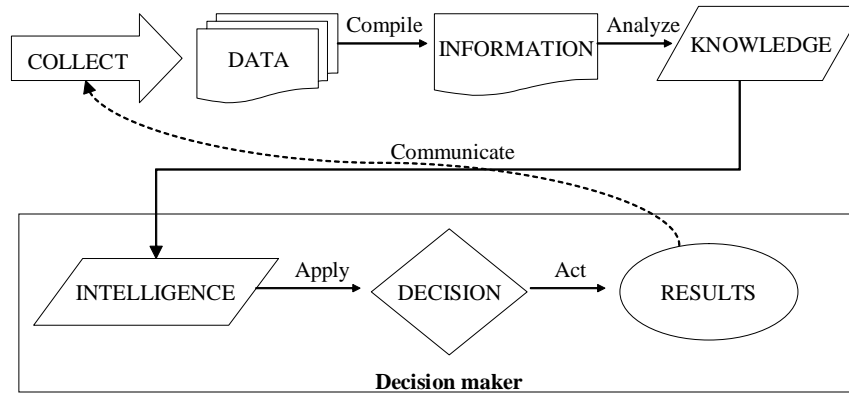
Moorman (1995) noted that organizational information process encompasses information acquisition, information transmission, conceptual utilization, and instrumental utilization. The goal of CI is to provide data that can respond to questions about opportunities and threats. Burwell (2004) described the advantages of using CI to include the transformation of a firm weaknesses into opportunities, predicting competitors' next strategic moves, gaining knowledge of environmental changes before it is too late to respond, mitigating and managing potential threats/risks proactively, achieving sustainable advantage, and dominating rivals in the marketplace. Two key factors that can influence the competitive advantage of any firm are endogenous and exogenous environments. Although majority of the business intelligence capability are built around the endogenous environment, in order to gain sustainable competitive advantage, organizations are expected to understand both the endogenous and exogenous environment (Oguz, 2002). According to (Oguz, 2002), if understanding endogenous and exogenous environments is the prerequisite to achieving strategic advantage, then the business intelligence capabilities must capture both the endogenous and exogenous data. Doner (2005) note that business intelligence capabilities are vital to enhancing forecast accuracy, operational productivity and customer demand management.

Because the current day operating environment has become very turbulent and thus risky, supply chain executives must rely on the external environment to access critical data to achieve actionable intelligence. However, Dugal and Prescott (1998) contend that access to information can only lead to an advantage if an organization is able to compile, interpret and disseminate that information to the decision makers on real-time fashion. CI function and CI process in Figure 1 depicts the development of actionable intelligence.

Essentially, the collected data is compiled to develop information which is analyzed to generate knowledge. And when that knowledge is communicated to decision makers it becomes intelligence necessary for action and results (Society of Competitive Intelligence Professionals, www.scip.org; Vibert, 2000).

Porter (1998) asserted that "gathering data is a waste of time unless they are used in formulating [corporate] strategy." Prescott (1999) emphasized that "a value-adding competitive intelligence process is a series of systematic organizational activities that are driven by specific [actionable] intelligence needs within the firm with the objective of achieving [sustainable]

Figure 1: CI Process Adapted from SCIP and William Y. Wilson, NextStep and Timothy W. Powell, InfoStrat



competitive advantage. Thus, supply chain executives who base their decisions on actionable intelligence will gain positional or differential advantage over rivals who do not use CI process as a core capability. It can help an organization identify managerial blind-spots (Gilad, 1994; Zahra and Chaples, 1993; Zajac and Bazerman, 1991). CI process entails the development of intelligence products, their dissemination on real-time bases, and the incorporation of such intelligence into the decision making process (Prescott, 1999). Also, CI is the process of monitoring the external or the competitive environment for early warning of surprises or disruptive risks. Andrews (1987) asserts that one of the main tenets of strategic planning is relationships between an organization and its environment that can influence its performance. "...knowing the [external or] competitive environment...will give risk managers a sense of intelligence on the risk exposure and the probability of the realization of risk. These will give them ability to plan, and act on it – manage risk" (Froilan).

COMPETITIVE INTELLIGENCE FOR SCRM

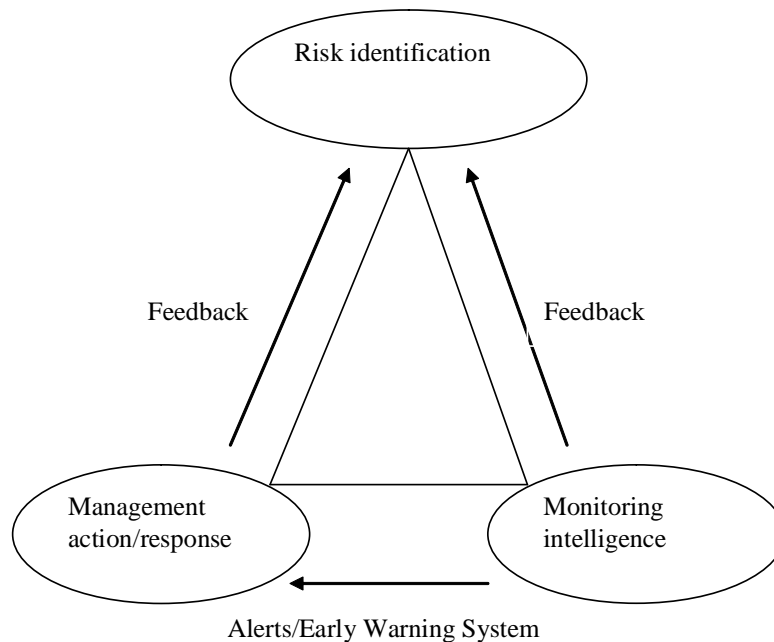
Supply Chain Blind Spots and Competitive Early Warning System

Gilad (1994) describes business blind spots as unchallenged assumptions, corporate myths, and corporate taboos that can cause competitive disadvantage. Unchallenged assumptions are those associated with the social, political, economic, competitive, suppliers, consumers' expectations, etc. Corporate myths represent the assumptions of how an organization feels about itself such as the feeling of invisibility which can be harmful to its competitiveness. Corporate taboos can entail a situation where a firm assumes it understands its operational environment, supply chain partners in particular. Blind spot behaviors are unconscious, negative actions often triggered by external events. To gain advantage, organizations must correct competitive blind spots that can lead to disaster to their operational efficiency and effectiveness. Organizations neglecting intelligence and complacent to the blind spots, do so to their detriment. Indeed, surprises can be a disruptive event for an organization when it fails to understand what is happening within and across the supply chains.

Brown and Weiner (1985) described early warning as a radar that constantly scan the environment and alert the new, the unexpected, the major and the minor surprises or threats. The competitive intelligence serves as early warning system or alerts to environmental threats. The competitive early warning system as shown in Figure 1 acts like a dashboard that is constantly monitoring, analyzing, and responding proactively to patterns and trends that can lead to potential opportunities and/or preempting potential supply chain disruptions. The competitive early warning system framework encompasses the identification of potential supply chain risks (threats) and/or opportunities; intelligence monitoring for warnings signs; and supply chain risk management action. The interdependent and convoluted nature of global supply chains in the current day operational environment has become vulnerable to disruptive risks. To carryout a successful SCRM, identification of portfolio of risks is imperative (Norrman and Lindroth, 2004; Hallikas *et al.*, 2002; Zoya and Russell, 2003). Although risk identification exercise is difficult because of the complexity and robustness of the global supply chain network, “unidentified risks may misguide supply chain risk management process (i.e., risk mitigation plan development), leading to inadequate or no appropriate strategies to control these risks and it could lead to major lost” (Karningsih *et al.*, 2007). SCRM encompasses identification of risk types and sources, risk analysis, risk evaluation and risk mitigation.

Risk Identification: to effectively mitigate and manage risks a firm must identify portfolio of risks. Some streams of research on identification of portfolio of risks include (Wu *et al.*, 2006; Kiser and Cantrell, 2006; Christopher and Peck, 2004; Cavinator, 2004; Chopra and Sodhi, 2004; Gaonkar, 2004; Hauser, 2003; Juttner *et al.*, 2003; Harland, *et al.*, 2003; Zsidisin, *et al.*, 2000)

Figure 2: The Competitive Intelligence Warning triangle



Adapted from Gilad, B. 2004. *Early Warning – Using Competitive Intelligence to Anticipate Market Shifts, Control Risk, and Create Powerful Strategies*. Amacom, New York.

Intelligence Monitoring (risk analysis and evaluation): The essence of supply chain intelligence monitoring is to make sense of the identified threats risk to avert any supply chain disruptions.

Management Response (risk mitigation): In this phase actionable information must be handed over to the appropriate decision makers to be able to respond proactively near real-time to the warning signs the environmental intelligence monitoring.

The current day tumultuous market conditions and competitive environment have raised the stakes for supply chain C-level executives, and managing supply chain risks through CI is poised to change the battleground for gaining competitive edge. To be successful, organization must radically change the way they sense, think, interpret and react (IBM Business Consulting, 2003) to potential opportunities and threats. According to Sun Tzu's Art of War, "If you know the enemy and know yourself, you need not fear the results of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself you will succumb in every battle." This statement is very relevant today for the forward-thinking organizations who must gain actionable intelligence through real-time knowledge to proactively respond to potential opportunities and threats in their operating environment. Thus, supply chain c-level executives "... have to be able to see past curves in the road to successfully maneuver around what lies ahead" (IBM Business Consulting, 2003) because those who "... have been hugely successful...are great not because they were focused on cost or flexibility or speed, but because they have the ability to manage transitions, changing market conditions, evolving technology, and different requirements as a product moves through its life cycle. The companies that can adapt are the ones that will be here for the long term" (Scott *et al.*, 2003). With CI capability firms can afford to respond with agility and speed to business environment opportunities and threats. Because supply chains have become more global and complex, CI is critical to a firm's ability to mitigate and manage risk. Gilad (1988) noted the possible areas of CI coverage as including competitors, growth opportunities, markets, technological, political, economic and social environments, demographics, suppliers and acquisition candidates.

Although CI tool has been used for supporting risk management endeavors in other fields, there is little or no application in SCRM. Based on review of relevant literature, only two studies discussed risk management using competitive intelligence. For example, Froilan used Fuld's intelligence cycle model as well as risk diagnostic hypothesis tree to examine financial risk management in banking industry in the Philippines. Vibert (2006) discussed leveraging online competitive intelligence to identify, assess and map organizational risks in order to develop actionable intelligence necessary for decision makers to achieve actionable results. Karningsih *et al.* (2007) discussed using knowledge based systems to assist in identifying potential risks and establish the interrelationships between risks in a supply chain network. There have been quite a number of other studies that have knowledge base system to identify and management risks in projects (e.g., Niwa 1989; Ramamoorthy *et al.*, 1993; Zoyza and Russel, 2003). Similarly, to enhance risk identification and management in construction

management, Ashley and Perng (1987) created an intelligent risk identification system through the integration of expert system, database management, and influence diagram representation.

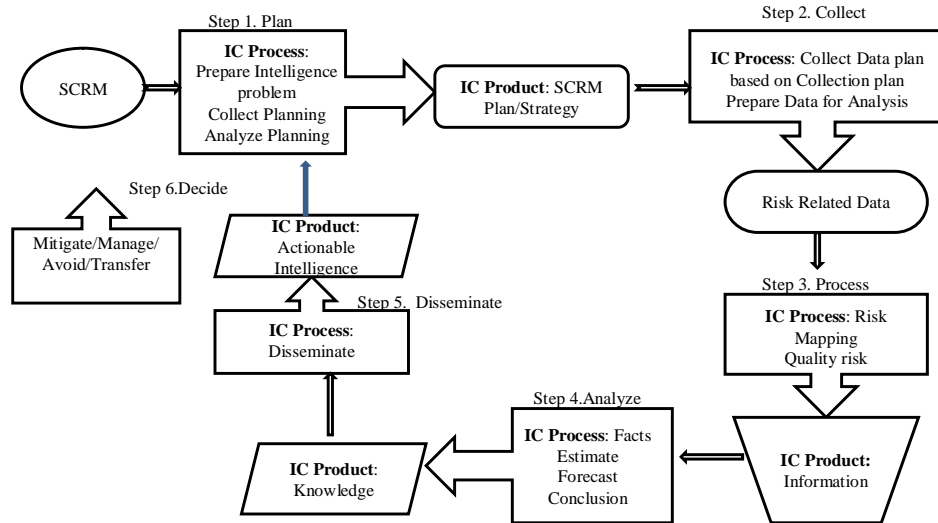
To decrease costs, grow revenues, and achieve sustainable advantage is the focus of CI-based SCRM. Essentially, the essence of CI-based SCRM is to create a supply chain CI that is vital to reducing overall supply chain costs, inventory carrying costs and order fulfillment. Supply chain risk comes in many different forms and from a variety of sources. Macroeconomic risk consists of market risk, interest-rate risk, currency risk, credit risk, and liquidity risk (Dorfman, 1994). Dorfman (1994) recommended steps for risk management include identification, evaluation, development, and selection of methods for managing risk.

Intelligence Cycle for Supply Chain Risk Management

Intelligence is the process of gathering, processing, reporting, and disseminating finished, actionable intelligence to decision makers. The goal of intelligence is to provide guidance that depends on appropriate and available information within a timeframe that can support purposeful action (Willis, 2007). The intelligence production process or the so called intelligence cycle (IC) contains all the variables needed to develop actionable CI. Miller (2000) identified the four phases of CI, including identification of key decision makers (e.g., chief risk officers) and their intelligence; information acquisition; analysis of information and upgrading it to actionable intelligence; and dissemination of the actionable intelligence to decision makers. According to Froilan, “the most important aspect of [SCRM] is to provide [supply chain] risk managers and risk takers an effective system, that will help them understand the nature of risk, communicate the risk, ways to monitor the cause and effects of risk and ...create strategic plan on how to prevent or manage risk.” Because identification of risks in modern global supply chains is a daunting challenge, there is a good chance that some risks will be left unnoticed. In view of this circumstance, the present paper utilizes CI process in Figure 3 to identify and manage risk in supply chain. Indeed, following Froilan, the present paper employs a combination of Fuld’s intelligence cycle and risk diagnostic hypothesis to identify, mitigate and manage supply chain risk. Kahaner, 1996; Ashton and Stacey, 1995; and Flud, 1995 consider CI process to consist of planning and direction, collection of data or information, process analysis, dissemination, and securitization. Thus, the IC-based SCRM encompasses planning and direction of intelligence collection of data/information (phase 1) that results in collection of new information (phase 2) that must be processed (phase 3), analyzed (phase 4), disseminated (phase 5) (Willis, 2007), and decided/acted on.

Adapted and modified from Froilan, S. “Competitive Intelligence Approach to Financial Risk Management in Banking”, <http://www.ermssymposium.org/2007/pdf/papers/Sia.pdf>.

The primary purpose of the CI in support of supply chain management is to enable continuous intelligence assessments concerning the strengths and weaknesses of competitors. The application of the CI within SCRM will be organized around the core intelligence process, the IC. The IC describes the steps used to create intelligence product. IC is an iterative process of planning and direction, collection of data, processing, analyses, and Dissemination. Intelligence processes exist to meet the actionable intelligence/ information requirements of decision makers such as the supply chain managers. Information gaps are identified and

Figure 3: SCRM Process using Intelligence Cycle to Develop Actionable Intelligence

collection assets are tasked to collect the necessary information. While some of the information that is collected may be fed directly from sensor to shooter, the supply chain manager's intelligence requirements can only be met by processing the collected information to produce actionable/information intelligence assessments. The resulting intelligence assessment must then be disseminated in a timely manner, in an appropriate form and by suitable means to those who need it. Speed of transmission and ease of comprehension on receipt are critical factors. According to Willis (2007), "intelligence is more valuable of the intelligence cycle operates faster than the opponent's. More rapid intelligence enables faster recognition of new threats and adaptation to shifts in opponents' strategies. Thus, methods to improve the accuracy and speed of the process provide a strategic advantage in efforts to combat..." threats.

Phase 1: Planning

Froilan suggests that the planning phase commences with risk identification to delivering intelligence product to an end user for the purpose of identifying, evaluating, monitoring, and controlling risk. Further, planning encompasses the entire intelligence process, commencing with the risk assessment phase and culminates with the delivery of the finished intelligence products. It formulates the appropriate actions to address specific portfolio of risks and prioritizing risk actions for integrated SCRM plan/strategy. The SCRM strategy can be in the form of mitigating and managing risk through logistics contingency planning, avoidance, transfer, compromise and/or accepting the risk. Plans generated must be responsive to the anticipated intelligence requirements. Planning at this phase integrates personnel, processes and tools using multiple information sources and collaborative analysis to build shared knowledge of the environmental factors. Information can be sourced from a wide range of sources, including intelligence, academia, industry, the public domain and other such non-traditional sources.

Phase 2: Data Collection

Effective data collection and real-time responsiveness to intelligence requirements is vital to supply chain decision makers. The capacity of the intelligence system to support decision makers effectively will depend on detailed initial analysis and the comprehensive planning of intelligence collection operations.

The collection requirement specifies exactly how the intelligence agent will go about procuring the intelligence information the decision maker requires. Collection requirements management requires analytic skill to evaluate how well the user has expressed the need; whether the collection assets are able to obtain the identified information, and how the collected information reaches the intelligence analyst.

Information from open sources are often a valuable collection resource in the business environment, including corporate publications, advertising, newspapers, periodicals, academic journals, foreign and domestic, official documents and other published material.

In the intensely competitive global economy today, acquiring information from environmental sources has become increasingly important for C-level executives.

Phase 3: Information Processing

The intelligence information must in an easy form to understand. Intelligence processes exist to meet the actionable intelligence/information of the decision markers such as the supply chain managers.

Phase 4: Analyze

Analysis is the transformation of supply chain risk data into actionable intelligence or supply chain risk decision-making information. Analysis provides the opportunity for the decision maker to pursue the appropriate and most critical risks. The collected information or data is analyzed to determine the extent to which they confirm, supplement, or contradict each other, and thus establish probabilities, relationships, and conclusions. The collected information is organized into a responsive intelligence product. The purpose of intelligence analysis is to provide the underlying significance of selected target information. Frequently intelligence analysis involves estimating one possible outcome, given the many possibilities in a particular scenario. The analysis typically can involve forecasting, which requires the analyst to make explicit statements about the degree of confidence held in a certain set of judgments. In intelligence analysis, the risk manager or chief risk officer gathers information from a variety of sources then proceeds to generating tentative explanations for risks (opportunities and threats). Each hypothesis is examined for answers and compared against the procured information for decision making.

Phase 5: Disseminate Intelligence

Supply chain risk dissemination emphasizes its pervasiveness and criticality in operating environment. SCRM cannot be achieved without effective dissemination of actionable intelligence regarding potential opportunities and threats. Indeed, for supply chain risks to be

analyzed and decisively managed, portfolio of risks must be disseminated within and across supply chain partners. The production of intelligence is valueless unless it is disseminated in real-time time to the decision maker and in a form that permits exploitation of the actionable intelligence. For actionable intelligence, it demands expedited production and dissemination of that intelligence for action. Nevertheless, the intelligence process never terminates with the product delivery to the decision maker. Rather, the intelligence process dialogue continues between producer and the decision, the end user. Indeed, for the product to be of value, dissemination must involve feedback. Feedback is crucial because decision makers need to know what is of value in order to meet the intelligence requirements necessary to respond to potential opportunities and threats.

Phase 6: Decide/Act

Supply chain risks must be identified before they can be mitigated and/or managed. Essentially, every type of risk must be explored before attempting to treat risks. In this phase, there is a requirement to “monitor the performance measures, record incidents and outcomes, and track changes in business or risk landscape. The information feeds back into step [or phase] one to complete virtuous circle. Indeed, monitoring serves as the “watchdog” that tracks the situation of supply chain risks and the SCRM strategies deployed to mitigate and manage them. In essence, portfolio of risks are identified and monitored to enhance the evaluation of the risk mitigation plans. Further, control is vital in this phase in order to correct anomalies or variations from risk mitigation planned actions. Risk control relies on decision makers to control risk action plans, correcting for anomalies or deviations from plans, responding to triggering risks, and improving SCRM processes.

CONCLUSIONS AND IMPLICATIONS

The need to gain competitive edge in current day ultra-competitive environment is pushing SCRM issues up the corporate agenda. As a result, C-level executives are increasingly demanding a SCRM strategy from their top supply chain managers. More than ever global supply chains are exposed to risks, including regulatory compliance, exchange rate fluctuation, interest rate, inflation rate, tariffs or duty rates, price of commodity, quality labor availability, labor union strike, political conditions, terrorism, natural disasters, and supply chain infrastructure. Those firms that can manage supply chain risks will create shareholder value and gain the Wall Street confidence. Those firms that neglect to respond to the call for action to implement SCRM do so at their own peril. According to McBeath (2004) “understanding the risks and managing to avert them can prevent unplanned cost and improve total performance. As the inevitable disruptions occur every day in supply chains (as in life), those that are the most resilient will win by a long shot.” Organizations have a responsibility to shareholders and consumers to pursue SCRM implementation.

A significant number of organizations are turning to CI more than ever because of globalization, information overload, ultra-competitiveness of new competitors, geopolitical and technological changes, and global supply chain disruptions. To pursue SCRM implementation, firms must urgently begin to place more emphasis on supply chain CI. Supply chain CI will enable a firm build world-class supply chain, respond dynamically and fast to

environmental risks such as intellectual property rights piracy, changes in customer demand, supply fluctuations, exchange fluctuation, high energy cost, among many others. Arguably, Supply Chain CI can be a vital source of value if organizations are able to capture, share, and leverage actionable information across supply chains. For supply chain executives, the ability to capture and share actionable information through CI is imperative to mitigating and managing supply chain risk. In essence, the ability to extract aggregated data that captures a complete view of the global business environment is essential if supply chain leaders are to respond proactively to opportunities and threats. So, they understand the know-how of finding, sharing, and using actionable information from external environment to effectively manage the associated risks and monitor their business operations. Hence in the current day risk laden operating environment, effectively managing risks within and across supply chains demands flow of information that is anchored on CI.

Further, the success of CI depends on three core business activities, including monitor – constantly and accurately monitoring activities in the environment and comparing such activities to historical activities or plans. Accurate monitoring of the operation environment provides firms with the comprehensive view of the actionable information they need to gain competitive advantage; analyze – examining the information obtained during the monitoring period enhances the actionable insight necessary to respond to opportunities and threats. A firm can transform that information into forward-looking actionable insight needed to take the opportunities and/or mitigate and manage ensuing risks; and plan – forecasting, planning, comparing plans to actual, analyzing that information, making the necessary adjustments, and taking appropriate action that matches the opportunities and/or threats.

Achieving sustainable competitive edge demands access to accurate and timely information and exploiting that information to mitigate risks. And one best means to gain access to an uninterrupted and reliable flow of actionable information about the macroeconomic environment is through CI. Those organizations that can successfully leverage CI to manage supply chain risks will gain sustainable competitive advantage and prosper. However, in spite of its successful application in other business fields, the concept of CI has attracted little or no attention of supply chain C-level executives. For supply chain C-level executives, the ability to leverage competitive intelligence is imperative to managing and mitigating portfolio of risks prevalent in today's global marketplace. Given today's brittle nature of global supply chains, CI is necessary ingredient to the success of any early warning function. CI can support organizations that desire survival and prosperity to evaluate their strengths and weaknesses to achieve supply chain CI intelligence (Wilkins, 2007). Supply chain CI is a process that adopts the discipline and ethics of competitive intelligence to enhance the supply chain operational efficiency and effectiveness.

References

- Andrews, K. R. (1987), *The Concept of Corporate Strategy*, 3rd Edition in *Leveraging Information for Action*. Homewood, IL: Richard D. Irwin.
- Adams, J. (1995), *Risk*. Routledge: London.
- Aberdeen Group (2006), "Global Supply Chain Benchmark Report: Industry Priorities for Visibility, B2B Collaboration, Trade Compliance, and Risk Management", www.aberdeens.com, pp. 1-31.

- Ashton, W. B. and Stacey, G. S. (1985), "Technical Intelligence in Business: Understanding Technology Threats and Opportunity", *International Journal of Technology Management, Special Issue on the Management of Technological Flows Across Boundaries*, Vol. 10, No. 1, pp. 79-104.
- Bandyopadhyay, K., Mykytyn, P. and Mykytyn, K. (1999), "A framework for Integrated Risk Management in Information Technology", *Management Decision*, Vol. 37, No. 5, pp. 437-44.
- Barry, J. (2004), "Supply Chain Risk in an Uncertain Global Supply Chain Environment", *International Journal of Physical Distribution & Logistics Management*, Vol. 34, No. 9, pp. 695-697.
- Bosman, R. (2006), "The New Supply Chain Challenge: Risk Management in a Global Economy", www.fmglobal.com, Global, pp. 1-10.
- Buehler, K. S. and Pritsch, G. (2003), "Running with Risk", *The McKinsey Quarterly*, No. 4, pp. 40-49.
- Burwell, H. P. (2004), *Online Competitive Intelligence*, Tempe, AZ: Facts on Demand Press.
- Cavinato, J. L. (2004), "Supply Chain Logistics Risks: From the Back Room to the Board Room", *International Journal of Physical Distribution & Logistics Management*, Vol. 34, No. 5, pp. 383-387.
- Chopra, S. and Sodhi, P. (2004), "Managing Risk to Avoid Supply Chain Breakdown", *MIT Sloan Management Review*, Vol. 46, No 1, pp. 53-61.
- Chopra, S. and Meindl, P. (2001), *Supply Chain Management: Strategy, Planning and Operation*, Prentice-Hall, Upper Saddle River, New Jersey.
- Christopher, M. and Peck, H. (2004), "Building the Resilient Supply Chain", *The International Journal of Logistics Management*, Vol. 15, pp. 1-13.
- Christopher, M. and Lee, H. (2004), "Mitigating Supply Chain Risk through Improved Confidence", *International Journal of Physical Distribution & Logistics Management*, Vol. 4, No. 5, pp. 388-396.
- Christopher, M. and Lee, H. (2001), *Supply Chain Confidence*, Working Paper, Cranfield School of Management, UK.
- Christopher, M. (2003), "Creating Resilient Supply Chains: A Practical Guide", www.cranfield.ac.uk/som/scr, pp. 1-100.
- Christopher, M. (2003), "Understanding Supply Chain Risk: A Self-Assessment Workbook", www.cranfield.ac.uk/som/scr, pp. 1-48.
- Courtney, H. (2001), "Making the Most of Uncertainty", *The McKinsey Quarterly*, No. 4, pp. 3847.
- Deleris, L. A. and Erhun, F. (2005), "Risk Management in Supply Networks Using Monte-Carlo Simulation", *Proceedings of the 2005 Winter Simulation Conference*, pp. 1643-1649.
- Deloitte (2004), "Supply Chain Risk Management", http://www.deloitte.com/dtt/cda/doc/content/nl_eng_brochure_supply_chain_risk_management_070704x%281%29.pdf.
- Dorfman, S. (1994), *Risk Management & Insurance* 5 ed., Englewood, N.J.: Prentice Hall.
- Doner, M. (2005), "Supply Chain Intelligence: Using Information as your Competitive Advantage", http://findarticles.com/p/articles/mi_qa5357/is_200511/ai_n21383599/print?tag=artBody;coll.
- Drucker, P. F. (1962), "The Economy's Dark Continent", *Fortune*, April, p. 103.
- Enyinda, C. I., Tolliver, D., and Szmerekovsky, J. (2007), "Mitigating and Managing Global Supply Chain Risks and Security: Leveraging RFID Technology", *In Proceeding of the Society for Advancement of Management*.
- Faisal, M. N. Banwet, D. K. and Shanker, R. (2006), "Supply Chain Risk Mitigation: Modeling the Enablers", *Business Process Management Journal*, Vol. 12, No. 4, pp. 535-552.

- Faisal, M. N., Banwet, D. K. and Shanker, R. (2007), "Quantification of Risk Mitigation Environment of Supply Chains using Graph Theory and Matrix Methods", *European Journal of Industrial Engineering*, Vol. 1, No. 1, pp. 22-39.
- Finch, P. (2004), "The Supply Chain Risk Management", *Supply Chain Management: An International Journal*, Vol. 9, No. 2, pp. 183-196.
- Froilan, S. "Competitive Intelligence Approach to Financial Risk Management in Banking", <http://www.ermssymposium.org/2007/pdf/papers/Sia.pdf>.
- Fuld, L. (1995), *The New Competitor Intelligence*. New York: Wiley.
- Gaonkar, R. and Viswanadham, N. (2004), "A Conceptual and Analytical Framework for the Management of Risk in Supply Chain", In the *Proceedings of the 2004 IEEE International Conference on Robotic and Automation*. New Orleans, USA.
- Gilad, B. (1994), *Business Blind Spots: Replacing your Company's Entrenched and Outdated Myths, Beliefs, and Assumptions with the Realities of Today's Markets*. Chicago: Probus.
- Goshal, S. and Westney, D. (1991), "Organizing Competitor Analysis Systems", *Strategic Management Journal*, Vol. 12, pp. 17-31.
- Griffith, S. E. (1971), *Sun Tzu: The Art of War*, New York, Oxford University Press.
- Hallikas, J. Virolainen, V. and Tuominen, M. (2002), "Risk Analysis and Assessment in Network Environments: A Dyadic Case Study", *International Journal of Production Economics*, Vol. 78, No. 1, pp. 45-55.
- Harland, C., Brenchley, R. and Walker, H. (2003), "Risk in Supply Networks", *Journal of Purchasing and Supply Management*, Vol. 9, No. 1, pp. 51-62.
- Heinrich, C. and Betts, B. (2003), *Adapt or Die: Transforming your Supply Chain into an Adaptive Business Network*, John Wiley & Sons, Inc.
- Hendricks, K. B. and Singhal, V. R. (2005), "An Empirical Analysis of the Effect of Supply chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm", *Production and Operations Management*, Vol. 14, No. 1, Spring, pp. 35-52.
- Hendricks, K. B. and Singhal, V. R. (2003), "The Effect of Supply Chain Glitches on Shareholder Wealth", *Journal of Operations Management*, Vol. 21, pp. 501-522.
- Holton, G. A. (2004), "Defining Risk", *Financial Analysts Journal*, Vol. 60, No. 6, pp. 19-25.
- IBM Business Consulting (2003), "Transforming your Supply Chain to on Demand: Competitive Advantage or Competitive Necessity"?
- Juttner, U., Peck, H. And Christopher, M. (2003), "Supply Chain Risk Management: Outlining an Agenda for Future Research", *International Journal of Logistics: Research and Applications*, Vol. 6, No. 4, pp. 197-210.
- Kahaner, L. (1996), *Competitive Intelligence: From Black Ops to Boardrooms, How Business Gather, Analyze, and Use Information to Succeed in the Global Marketplace*, New York: Simon and Schuster.
- Karningsih, P. D., Kayis, B., and Kara S. (2007), "Development of Knowledge Based Systems for Supply Chain Risk Identification in Multi-Site & Multi-Partners Global Manufacturing Supply Chain", In the *Proceedings of the 13th Asia Pacific Management Conference*, Melbourne, Austria, pp. 466-471.
- Kleindorfer, P. R. and Van Wassenhove, L. N. (2004), "Managing Risk in Global Supply Chains", in H. Gatignon and J. Kimberly (eds.), *The Alliance on Globalization*, Cambridge University Press.

- Kleindorfer, P. R. and Saad, G. H. (2005), "Managing Disruption Risks in Supply Chains", *Production and Operations Management*, Vol. 14, No. 1, Spring, pp. 53-68.
- Kleindorfer, P. R. (2000), "Industrial Ecology and Risk Analysis", <http://grace.wharton.upenn.edu/risk/downloads/01-25-pk.pdf>.
- Lamming, R., Caldwell, N., Harrison, D. and Phillips, W. (2001), "Transparency in Supply Relationships: Concept and Practice", in the *Proceedings of the 10th International IPSE Conference*, pp. 585-94.
- Lindroth, R. and Norman, A. (2001), "Supply Chain Risks and Risk Sharing Instruments: An Illustration from the Telecommunication Industry", in the *Proceedings of the Logistics Research Network 6th Annual Conference*, Heriot-Watt University, 13-14 September, pp. 297-307.
- March, J. and Shapira, Z. (1987), "Managerial Perspectives on Risk and Risk Taking", *Management Science*, Vol. 33, No. 11, pp. 1404-1418.
- McBeath, B. (2004), "Resilient Supply Chains – The Next Frontier", chainlinkresearch.com/research/detail.cfm?...
- McGonagle, J. J. and Vella, V. E. (2002), "A Case for Competitive Advantage", *The Information Management Journal*, Jul/August, pp. 35-40.
- Miller, J. (2000), *Millennium Intelligence*, Medford, NJ: Cyber Age Books.
- Moorman, C. (1995), "Organizational Market Information Process: Cultural Antecedents and New Product Outcomes", *Journal of Marketing Research*, Vol. 32, pp. 318-335.
- Norrman, A. and Lindroth, R. (2004), Categorization of Supply Chain Risk and Risk Management, in Brindley, C. (Ed.) *Supply Chain Risk*. Hampshire, England, Ashgate Publishing Ltd.
- Moschini, G. and Hennessy, D. A. (1999), "Uncertainty, Risk Aversion and Risk Management for Agricultural Producers", in Bruce Gardner and Gordon Rausser, Eds., *Handbook of Agricultural Economics*, Amsterdam: Elsevier Science Publishers.
- Murphy, J. (2006), "Managing Supply Chain Risk: Building in Resilience and Preparing for Disruption", http://www.wisdomnet.net/documents/whitepapers/SCM_Risk_2006.pdf.
- Niwa, K. (1989), *A Knowledge-Based Risk Management in Engineering in United States*, John Wiley & Sons Inc.
- Norrman, A. and Jansson, U. (2004), "Ericsson's Proactive Supply Chain Risk Management Approach After a Serious Sub-Supplier Accident", *International Journal of Physical Distribution & Logistics Management*, Vol. 34, No 5, pp. 434-456.
- O'Brien, P. and Joyce, G. (2007), "Risk Management: Supply Chain Risk – Are you the Weakest Link?", <http://www.linkresq.ie/papers/Risk%20Management%20-%20Supply%20Chain%20Risk.pdf>, pp. 1-6.
- Peck, H. (2006), "Reconciling Supply Chain Vulnerability, Risk and Supply Chain Management", *International Journal of Logistics: Research and Applications*, Vol. 9, No. 2, pp. 127-142.
- Oguz, M. T. (2002), "Business Intelligence in Competitive Strategy", http://www.dmreview.com/news/5601-html?type=printer_friendly.
- Porter, M. (1998), *Competitive Strategy*, NY: The Free Press.
- Porter, M. E. and Miller, V. E. (1985), "How information Gives You Competitive Advantage", *Harvard Business Review*, Vol. 63, No. 4, pp. 149-160.

- Prescott, J. E. "The Evolution of Competitive Intelligence: Designing a Process for Action", <http://www.apmp.org/fr-154.aspx>.
- Prescott, J. E. and Gibbons, P. (Eds.). (1993), *Global Perspectives on Competitive Intelligence*, Alexandria, VA: Society of Competitive Intelligence Professionals (SCIP).
- Ramamoorthy, C. V., Chandra, C., Ishihara, S. and Ng, Y. (1993), "Knowledge Based Tools for Risk Assessment in Software Development and Reuse", 1993 IEE International Conference on Tools with Artificial Intelligence, Boston, MA.
- Rice, J. B. and Caniato, F. (2003), "Building a Secure and Resilient Supply Network", *Supply Chain Management Review*, September/October, pp. 22-30.
- Sheffi, Y. and Rice, J. B. (2005), "A Supply Chain View of the Resilient Enterprise", *MIT Sloan Management Review*, Fall, Vol. 47, No. 1, pp. 41-48.
- Simchi-Levi, D., Snyder, L. and Watson, M. (2002), "Strategies for Uncertain Times", *Supply Chain Management Review*, January/February, pp. 11-12.
- Spekman, R. E. and Davis, E. W. (2004), "Risky Business: Expanding the Discussion on Risk and the Extended Enterprise", *International Journal of Physical Distribution and Logistics Management*, Vol. 34, No. 5, pp. 414-433.
- Van Landeghem, H. and Vanmaele, H. (2002), "Robust Planning: A New Paradigm for Demand Chain Planning", *Journal of Operations Management*, Vol. 20, pp. 769-83.
- Vibert, C. (2006), "Using Online Competitive Intelligence to Help Identify Organizational Risk", *The Workplace Review*, April, pp. 37-42.
- Willis, H. H. (2007), "Using Risk Analysis to Inform Intelligence Analysis", Working Paper, Rand Corporation, February, pp. 1-15.
- Wilkins, L. Richard (2007), "Competitive Intelligence: The New Supply Chain Edge", *Supply Chain Management Review* – http://www.scmr.com/index.asp?layout=articlePrint&articleID=CA6406211&article_prefi...
- Wu, T., Blackhurst, J. and Chidambaram, V. (2006), "A Model of Inbound Supply Risk Analysis", *Computers in Industry*, Vol. 57, pp. 350-365.
- Zahra, S. A. and Chaples, S. S. (1993), "Blind Spots in Competitive Analysis", *The Academy of Management Executive*, Vol. 2, pp. 7-28.
- Zajac, E. and Bazerman, M. (1991), "Blind Spots in Industry and Competitive Analysis: Implications of Inter-firm (Mis)perceptions for Strategic Decisions", *Academy of Management Review*, Vol. 16, pp. 37-56.
- Zoyza, S. D. and Russel, A. D. (2003), "Knowledge-Based Risk Identification in Infrastructure Projects", *Canadian Journal of Civil Engineering*, Vol. 30, pp. 511-522.
- Zsidisin, G. A., Ellram, L. M., Carter, J. R. and Cavinato, J. L. (2004), "Analysis of Supply Risk Assessment Techniques", *International Journal of Physical Distribution & Logistics Management*, Vol. 34, No. 5, pp. 397-413.
- Zsidisin, G. A., Panelli, A. and Upton, R. (2000), "Purchasing Organization Involvement in Risk Assessments, Contingency Plans, and Risk Management: An Exploratory Study", *Supply Chain Management*, Vol. 5, No. 4, p. 187.