Enterprise Risk Management in Supply Chains

1

All human endeavors involve uncertainty and risk. Mitroff and Alpaslan (2003) categorized emergencies and crises into three categories: natural disasters, malicious activities, and systemic failures of human systems.[1] **Nature** does many things to us, disrupting our best-laid plans and undoing much of what humans have constructed. Natural disasters by definition are surprises, causing a great deal of damage and inconvenience. Nature inflicts disasters such as volcanic eruptions, tsunamis, hurricanes and tornados. Guertler and Spinler[2] noted a number of supply chain disruptions in recent years due to natural causes. In 2007 an earthquake damaged Toyota's major supplier for key parts, leading to shutdown of Toyota's Japanese factories as well as impacting Mitsubishi, Suzuki, and Honda. In 2010 the Icelandic volcanic activity shut down European air space for about a week, massively disrupting global supply chains. In 2011 the tsunami leading to the Fukushima disaster disrupted automakers and electronic supply chains, as well as many others.

While natural disasters come as surprises, we can be prepared. Events such as earthquakes, floods, fires and hurricanes are manifestations of the majesty of nature. In some cases, such as Mount Saint Helens or Hurricane Katrina,[3] we have premonitions to warn us, but we never completely know the extent of what is going to happen. Emergency management is a dynamic process conducted under stressful conditions, requiring flexible and rigorous planning, cooperation, and vigilance.

Some things we do to ourselves, to include revolutions, terrorist attacks and wars. **Malicious acts** are intentional on the part of fellow humans who are either excessively competitive or who suffer from character flaws. Wars fall within this category, although our perceptions of what is sanctioned or malicious are colored by our biases. Criminal activities such as product tampering or kidnapping and murder are clearly not condoned. Acts of terrorism are less easily classified, as what is terrorism to some of us is expression of political behavior to others. Similar gray categories exist in the business world. Marketing is highly competitive, and positive spinning of your product often tips over to malicious slander of competitor

D.L. Olson, D.D. Wu, *Enterprise Risk Management Models*, Springer Texts in Business and Economics, DOI 10.1007/978-3-662-53785-5_1

products. Malicious activity has even arisen within the area of information technology, in the form of identity theft or tampering with company records.

The third category is probably the most common source of crises: **unexpected consequences arising from overly complex systems**.[4] Some disasters combine human and natural causes—we dam up rivers to control floods, to irrigate, to generate power, and for recreation, as at Johnstown, PA at the turn of the twentieth Century. We have developed low-pollution, low-cost electricity through nuclear energy, as at Three-Mile Island in Pennsylvania and Chernobyl. The financial world is not immune to systemic failure. Financial risk importance was evidenced traumatically by events of 2007 and 2008, when the global financial community experienced a real estate bubble collapse from which most of the world's economies are still recovering. Human investment activity seems determined to create bubbles, despite our long history of suffering.[5] Financial investment seems to be a never-ending game of greedy players seeking to take advantage of each other, which Adam Smith assured us would lead to an optimal economic system. It is interesting that we pass through periods of trying one system, usually persisting until we encounter failure, and then move on to another system.[6]

Unexpected Consequences

Charles Perrow contended that humans are creating technologies that are high risk because they are too complex, involving interactive complexity in tightly coupled systems. Examples include dam systems, which have provided a great deal of value to the American Northwest and Midwest, but which also create potential for disaster when dams might break; mines, which give access to precious metals and other needed materials but which have been known to collapse; and space activities, which demonstrate some of mankind's greatest achievements, as well as some of its most heartbreaking failures. Nuclear systems (power or weapon) and airline systems are designed to be highly reliable, with many processes imposed to provide checks and balances. Essentially, humans respond to high risk by creating redundant and more complex systems, which by their nature lead to a system prone to greater likelihood of systems failure.

Technological innovation is a manifestation of human progress, but efforts in this direction have yielded many issues. In the energy field, nuclear power was considered the solution to electrical supply 50 years ago. While it has proven to be a viable source of energy in France and other European countries, it has had problems in the US (Three Mile Island) and in the former Soviet Union (Chernobyl). There is a reticence on the part of citizens to nuclear power, and the issue of waste disposal defies solution. Even in Europe the trend is away from nuclear. The Federal Government in the US did not license new plants for decades, despite technological advances developed by national laboratories. Coal remains a major source of electrical energy fuel, although there are very strong questions concerning the need to replace it for carbon footprint reasons. Natural gas is one alternative. Wind power is another. Solar energy has been proposed. All of these alternatives

can be seen to work physically, if not economically. The question of energy was further complicated with the recent large-scale adoption of *fracking*. This technique introduces risk and uncertainty not only to itself, but its inclusion changes decision-making regarding all sectors of energy.

All organizations need to prepare themselves to cope with crises from whatever source. In an ideal world, managers would identify everything bad that could happen to them, and develop a contingency plan for each of these sources of crisis. It is a good idea to be prepared. However, crises by definition are almost always the result of nature, malicious humans, or systems catching us unprepared (otherwise there may not have been a crisis). We need to consider what could go wrong, and think about what we might do to avoid problems. We cannot expect to cope with every contingency, however, and need to be able to respond to new challenges.

Enterprise risk management, especially in finance and accounting,[7] is well-covered by many sources. This book will review the types of risks faced within supply chains as identified by recent sources. We will also look at project management, information systems, emergency management, and sustainability aspects of supply chain risk. We will then look at processes proposed to enable organizations to identify, react to, and cope with challenges that have been encountered. This will include looking at risk mitigation options. One option explored in depth will be the application of value-focused analysis to supply chain risk. We will then seek to demonstrate points with cases from the literature. We will conclude this chapter with an overview.

Supply Chain Risk Frameworks

There is a rapidly growing body of literature concerning risk management, to include special issues in Technovation,[8] Omega,[9] and Annals of Operations Research.[10] Special issues also have been devoted to sustainability and risk management.[11] This literature involves a number of approaches, including some frameworks, categorization of risks, processes, and mitigation strategies. Frameworks have been provided by many, to include Lavastre et al.[12] and Desai et al.[13] We begin with a general framework. Ritchie and Brindley[14] viewed five major components to a framework in managing supply chain risk.

Risk Context and Drivers

Supply chains can be viewed as consisting of primary and secondary levels. The primary level chain involves those that have major involvement in delivery of goods and services (Wal-Mart itself and its suppliers). At the secondary level participants have a more indirect involvement (those who supply vendors who have contracts with Wal-Mart, or Wal-Mart's customers). The primary level participants are governed by contractual relationships, obviously tending to be more clearly stated. Risk drivers can arise from the external environment, from

within an industry, from within a specific supply chain, from specific partner relationships, or from specific activities within the organization.

Risk drivers arising from the external environment will affect all organizations, and can include elements such as the potential collapse of the global financial system, or wars. Industry specific supply chains may have different degrees of exposure to risks. A regional grocery will be less impacted by recalls of Chinese products involving lead paint than will those supply chains carrying such items. Supply chain configuration can be the source of risks. Specific organizations can reduce industry risk by the way the make decisions with respect to vendor selection. Partner specific risks include consideration of financial solvency, product quality capabilities, and compatibility and capabilities of vendor information systems. The last level of risk drivers relate to internal organizational processes in risk assessment and response, and can be improved by better equipping and training of staff and improved managerial control through better information systems.

Risk Management Influencers

This level involves actions taken by the organization to improve their risk position. The organization's attitude toward risk will affect its reward system, and mold how individuals within the organization will react to events. This attitude can be dynamic over time, responding to organizational success or decline.

Decision Makers

Individuals within the organization have risk profiles. Some humans are more risk averse, others more risk seeking. Different organizations have different degrees of group decision making. More hierarchical organizations may isolate specific decisions to particular individuals or offices, while flatter organizations may stress greater levels of participation. Individual or group attitudes toward risk can be shaped by their recent experiences, as well as by the reward and penalty structure used by the organization.

Risk Management Responses

Each organization must respond to risks, but there are many alternative ways in which the process used can be applied. Risk must first be identified. Monitoring and review requires measurement of organizational performance. Once risks are identified, responses must be selected. Risks can be mitigated by an implicit tradeoff between insurance and cost reduction. Most actions available to organizations involve knowing what risks the organization can cope with because of their expertise and capabilities, and which risks they should outsource to others at some cost. Some risks can be dealt with, others avoided.

Performance Outcomes

Organizational performance measures can vary widely. Private for-profit organizations are generally measured in terms of profitability, short-run and long-run. Public organizations are held accountable in terms of effectiveness in delivering services as well as the cost of providing these services. Kleindorfer and Saad gave 8 key drivers of disruption/risk management in supply chains[15]:

Corporate image	Regulatory compliance
Liability	Community relations
Employee health and safety	Customer relations
Cost reduction	Product improvement

In normal times, there is more of a focus on high returns for private organizations, and lower taxes for public institutions. Risk events can make their preparation in dealing with risk exposure much more important, focusing on survival.

Cases

The research literature is very heavily populated by studies of supply chain risk in recent years. Diabat et al.[16] presented a model of a food supply chain with five categories (macro concerning nature and political, demand, supply, product, and information management) of risk using interpretive structural modeling. Hachicha and Elmasalmi[17] proposed structural modeling and MICMAC (cross-impact) analysis for risk prioritization. Aqlan and Lam[18] applied optimization modeling to mitigate supply chain risks in a manufacturing environment. Davarzani et al.[19] considered economic/political risk in three companies in the automotive field, while Ceryno et al.[20] developed risk profiles in terms of drivers, sources, and events for automotive cases in Brazil. Trkman et al.[21] surveyed 89 supply chain companies, finding a predominant focus on risk avoidance rather than using risk management for value generation. These cases cited are only the tip of the iceberg, meant to give some flavor of the variety of supply chain domains that have been analyzed for risk.

Models Applied

Many different types of models have been proposed in the literature. Because of the uncertainty involved, statistical analysis and simulation are very appropriate to consider supply chain risk. Bayesian analysis has been proposed to model supply chain risk.[22] Simulation was proposed in a number of studies, to include discrete-event simulation.[23] Colicchia et al.[24] applied simulation modeling to support risk management in supply chains. Simulation modeling of personnel system supply chains has been addressed.[25] System dynamics models have been widely used[26] and

with respect to the bullwhip-effect.[27] Other modeling approaches have been applied to supply chain risk as well.[28] Optimization is widely used,[29] and even data mining.[30]

Risk Categories Within Supply Chains

Supply chains involve many risks. Cucchiella and Gastaldi[31] divided supply chain risks into two categories: internal (involving such issues as capacity variations, regulations, information delays, and organizational factors) and external (market prices, actions of competitors, manufacturing yield and costs, supplier quality, and political issues). Specific supply chain risks considered by various studies are given in Table 1.1:

Supply chain organizations thus need to worry about risks from every direction. In any business, opportunities arise from the ability of that organization to deal with risks. Most natural risks are dealt with either through diversification and redundancy, or through insurance, both of which have inherent costs. As with any business decision, the organization needs to make a decision considering tradeoffs. Traditionally, this has involved the factors of costs and benefits. Society is more and more moving toward even more complex decision-making domains requiring consideration of ecological factors as well as factors of social equity.

Dealing with other external risks involves more opportunities to control risk sources. Some supply chains in the past have had influence on political systems. Arms firms like that of Alfred Nobel come to mind, as well as petroleum businesses, both of which have been accused of controlling political decisions. While most supply chain entities are not expected to be able to control political risks like wars and regulations, they do have the ability to create environments leading to labor unrest. Supply chain organizations have even greater expected influence over economic factors. While they are not expected to be able to control exchange rates, the benefit of monopolies or cartels is their ability to influence price. Business organizations also are responsible to develop technologies providing competitive advantage, and to develop product portfolios in dynamic markets with product life cycles. The risks arise from never-ending competition.

Internal risk management is more directly the responsibility of the supply chain organization and its participants. Any business organization is responsible to manage financial, production, and structural capacities. They are responsible for programs to provide adequate workplace safety, which has proven to be cost-beneficial to organizations as well as fulfilling social responsibilities. Within supply chains, there is need to coordinate activities with vendors, and to some degree with customers (supported by data obtained through bar-code cash register information providing instantaneous indication of demand). Information systems technology provides effective tools to keep on top of supply chain information exchange. Another factor of great importance is the responsibility of supply chain core

Table 1.1 Supply chain risk categories

Category	Risk	A	B	C	D	E	F	G
External								
Nature	Natural disaster: flood, earthquake	X	X		X		X	X
	Plant fire				X			
	Diseases, epidemics		X				X	
Political system	War, terrorism	X			X		X	
	Labor disputes	X	X		X		X	X
	Customs and regulations	X	X	X	X		X	X
Competitor and market	Price fluctuation			X				
	Economic downturn		X					
	Exchange rate risk	X			X			
	Consumer demand volatility		X	X		X		
	Customer payment	X						
	New technology		X	X				
	Obsolescence	X			X			
	Substitution alternatives				X			
Internal								
Available capacity	Cost	X	X					X
	Financial capacity/insurance		X	X				
	Structural capacity	X	X	X	X			X
	Supplier bankruptcy				X			X
Internal operation	Forecast inaccuracy	X	X		X			X
	Safety (worker accidents)		X				X	
	Agility/flexibility		X	X	X			
	On-time delivery		X		X			X
	Quality		X		X			X
Information system	IS breakdown	X						
	Integration	X			X		X	

A—Chopra and Sodhi (2004)[32]
B—Wu et al. (2006)[33]
C—Cucchiella and Gastaldi (2006)[34]
D—Blackhurst et al. (2008)[35]
E—Manuj and Mentzer (2008)[36]
F—Wagner and Body (2008)[37]
G—Lavastre et al. (2014)[38]

organizations to manage risks inherent in the tradeoff between wider participation made possible through Internet connections (providing a larger set of potential suppliers leading to lower costs) with the reliability provided by long-term relationships with a smaller set of suppliers that have proven to be reliable.

Process

A process is a means to implement a risk management plan. Cucchiella and Gastaldi outlined a supply chain risk management process[39]:

- **Analysis**: examine supply chain structure, appropriate performance measures, and responsibilities
- **Identify sources of uncertainty**: focus on most important
- **Examine risks**: select risks in controllable sources of uncertainty
- **Manage risk**: develop strategies
- **Individualize most adequate real option**: select strategies for each risk
- **Implement**

This can be combined with a generic risk management process compatible with those provided by Hallikas et al., Khan and Burnes, Autry and Bobbitt, and by Manuj and Mentzer[40]:

- **Risk identification**
  - Perceiving hazards, identifying failures, recognizing adverse consequences
  - Security preparation and planning
- **Risk assessment** (estimation) **and evaluation**
  - Describing and quantifying risk, estimating probabilities\
  - Estimating risk significance, acceptability of risk acceptance, cost/benefit analysis
- **Selection of appropriate risk management strategy**
- **Implementation**
  - Security-related partnerships
  - Organizational adaptation
- **Risk monitoring/mitigation**
  - Communication and information technology security

Both of these views match the Kleindorfer and Saad risk management framework[41]:

1. The initial requirement is to specify the nature of underlying hazards leading to risks;
2. Risk needs to be quantified through disciplined risk assessment, to include establishing the linkages that trigger risks;
3. To manage risk effectively, approaches must fit the needs of the decision environment;
4. Appropriate management policies and actions must be integrating with on-going risk assessment and coordination.

In order to specify, assess and mitigate risks, Kleindorfer and Saad proposed ten principles derived from industrial and supply chain literatures:

1. Before expecting other supply chain members to control risk, the core activity must do so internally;
2. Diversification reduces risk—in supply chain contexts, this can include facility locations, sourcing options, logistics, and operational modes;
3. Robustness to disruption risks is determined by the weakest link;
4. Prevention is better than cure—loss avoidance and preemption are preferable to fixing problems after the fact;
5. Leanness and efficiency can lead to increased vulnerability
6. Backup systems, contingency plans, and maintaining slack can increase the ability to manage risk;
7. Collaborative information sharing and best practices are needed to identify vulnerabilities in the supply chain;
8. Linking risk assessment and quantification with risk management options is crucial to understand potential for harm and to evaluate prudent mitigation;
9. Modularity of process and product designs as well as other aspects of agility and flexibility can provide leverage to reduce risks, especially those involving raw material availability and component supply;
10. TQM principles such as Six-Sigma give leverage in achieving greater supply chain security and reduction of disruptive risks as well as reducing operating costs.

Mitigation Strategies

There are many means available to control risks within supply chains. A fundamental strategy would be to try to do a great job in the fundamental supply chain performance measures of consistent fulfillment of orders, delivery dependability, and customer satisfaction. That basically amounts to doing a good job at what you do. Of course, many effective organizations have failed when faced with changing markets or catastrophic risks outlined in the last section as external risks. Some strategies proposed for supply chains are reviewed in Table 1.2:

Chopra and Sodhi developed a matrix to compare relative advantages or disadvantages of each strategy with respect to types of risks.[47] Adding capacity would be expected to reduce risk of needing more capacity of course, and also decrease risk of procurement and inventory problems, but increases the risk of delay. Adding inventory is very beneficial in reducing risk of delays, and reduces risk of disruption, procurement, and capacity, but incurs much greater risk of inventory-related risks such as out-dating, spoilage, carrying costs, etc. Having redundant suppliers is expected to be very effective at dealing with disruptions, and also can reduce procurement and inventory risk, but can increase the risk of excess

Table 1.2 Supply chain mitigation strategies

A	B	C	D	E
Add capacity			Expand where you have competitive advantage	
Add inventory	Buffers			Safety stock
Redundant suppliers	Multiple sources	Monitor suppliers	Drop troublesome suppliers	
Increase responsiveness	Information sharing	Contingency planning		End-to-end visibility
Increase flexibility	Product differentiation	Late product differentiation	Delay resource commitment	Supply flexibility
Pool demand				Multiple sourcing
Increase capability			Outsource low probability demand	
More customers				
	Early supplier involvement	Information sharing	Sharing/transfer	Awareness
	Risk taking	Insurance	Hedge (insure, disperse globally)	Supplier development
			Drop troublesome customers	

A—Chopra and Sodhi (2004)[42]
B—Khan and Burnes (2007)[43]
C—Wagner and Bode (2008)[44]
D—Manuj and Mentzer (2008)[45]
E—Oke and Gopalakrishnan (2009)[46]

capacity. Other strategies had no negative expected risk impacts (increasing responsiveness, increasing flexibility, aggregating demand, increasing capability, or increasing customer accounts), but could have negative cost implications. Talluri et al.[48] assessed such strategies via simulation.

Tang emphasized robustness.[49] He gave nine robust supply chain strategies, some of which were included in Table 1.2. He elaborated on the expected benefits of each strategy, both for normal operations as well as in dealing with major disruptions, outlined in Table 1.3, organized by purpose:

Cucchiella and Gastaldi gave similar strategies, with sources of supply chain research that investigated each.[50] Cucchiella and Gastaldi expanded Tang's list to include capacity expansion. Ritchie and Brindley included risk insurance, information sharing, and relationship development.[51]

Table 1.3 Tang's Robust supply chain strategies

Strategy	Purpose	Normal benefits	Disruption benefits
Strategic stock	Product availability	Better supply management	Quick response
Economic supply incentives			Can quickly adjust order quantities
Postponement	Product flexibility		Can change product configurations quickly in response to actual demand
Flexible supply base	Supply flexibility		Can shift production among suppliers quickly
Make-and-buy			Can shift production in-house or outsource
Flexible transportation	Transportation flexibility		Can switch among modes as needed
Revenue management	Control product demand	Better demand management	Influence customer selection as needed
Dynamic assortment planning			Can influence product demand quickly
Silent product rollover	Control product exposure	Better manage both supply and demand	Quickly affect demand

Conclusions

Enterprise risk management began focusing on financial factors. After the corporate scandals in the U.S. in the early 2000s, accounting aspects grew in importance. This chapter discusses the importance of risk management in the context of supply chain management.

A representative risk framework based on the work of Ritchie and Brindley was presented. It rationally begins by identify causes (drivers) of risk, and influencers within the organization. Those responsible for decision making are identified, and a process outlined where risks, responses, and measures of outcomes are included.

There have been many cases involving supply chain risk management reported recently. Some were briefly reviewed, along with quantitative modeling. Typical risks faced by supply chains were extracted from sources, and categorized. A process of risk identification, assessment, strategy development and selection, implementation and monitoring is reviewed. Representative mitigation strategies were extracted from published sources.

Chapter 2 addresses the enterprise risk management process, describing use of risk matrices. Chapter 3 describes value-focused supply chain risk analysis, with examples demonstrated in Chap. 4. Chapter 5 provides simulation modeling of supply chain inventory. Chapter 6 deals with value at risk, Chap. 7 with chance

constrained modeling, Chap. 8 with data envelopment analysis, and Chap. 9 with data mining from the perspective of enterprise risk management. Chapter 10 concludes the methods section of the book with balanced scorecards as tools to monitor implementation of risk management efforts. Domain specific issues for information systems are discussed in Chap. 11, for project management in Chap. 12, natural disaster response in Chap. 13, sustainability risk management in Chap. 14, and environmental damage and risk assessment in Chap. 15.

Notes

1. Mitroff, I.I. and Alpaslan, M.C. (2003). Preparing for evil, *Harvard Business Review* 81:4, 109–115.
2. Guertler, B. and Spinler, S. (2015). Supply risk interrelationships and the derivation of key supply risk indicators, *Technological Forecasting & Social Change* 92, 224–236.
3. Kapucu, N. and Van Wart, M. (2008). Making matters worse: An anatomy of leadership failures in managing catastrophic events, *Administration & Society* 40(7): 711–740.
4. Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press, 1999 reprint.
5. Laeven, L. and F. Valencia (2008) 'Systemic banking crises: A new database', International Monetary Fund Working Paper WP/08/224.
6. Wu, D.D. and Olson, D.L. (2015), *Enterprise Risk Management in Finance*. New York: Palgrave Macmillan.
7. Olson, D.L. and Wu, D.D. (2015). *Enterprise Risk Management 2nd ed.*. Singapore: World Scientific.
8. Olson, D.L., Birge, J. and Linton, J. (2014). Special issue: Risk management in cleaner production. *Technovation* 34:8, 395–398.
9. Wu, D.D., Olson, D.L. and Dolgui, A. (2015). Decision making in enterprise risk management. *Omega* 57 Part A, 1–4.
10. Wu, D. (2016). Risk management and operations research: A review and introduction to the special issue. *Annals of Operations Research* 237(1–2), 1–3.
11. Wu, D.D., Olson, D.L. and Birge, J.R. (2013). Risk management in cleaner production. *Journal of Cleaner Production* 53, 1–6.
12. Lavastre, O., Gunasekaran, A. and Spalanzani, A. (2014). Effect of firm characteristic, supplier relationships and techniques used on supply chain risk management (SCRM): An empirical investigation on French industrial firms. *International Journal of Production Research* 52(110), 3381–3403.
13. Desai, K.J., Desai, M.S. and Ojode, L. (2015). Supply chain risk management framework: A fishbone analysis approach. *SAM Advanced Management Journal* 80(3), 34–56.
14. Ritchie, B. and Brindley, C. (2007a). An emergent framework for supply chain risk management and performance measurement, *Journal of the Operational Research Society* 58, 1398–1411; Ritchie, B. and Brindley, C. (2007b). Supply

chain risk management and performance: A guiding framework for future development, *International Journal of Operations & Production Management* 27:3, 303–322.
15. Kleindorfer, P.R. and Saad, G.H. (2005). Managing disruption risks in supply chains, *Production and Operations Management* 14:1, 53–68.
16. Diabat, A., Govindan, K. and Panicker, v.V. (2012). Supply chain risk management and its mitigation in a food industry. *International Journal of Production Research* 50(11), 3039–3050.
17. Hachicha, W. and Elmsalmi, M. (2014) An integrated approach basedstruct6ural modeling rfor risk prioritization in supply network management. *Journal of Risk Research* 17(10), 1301–1324.
18. Aqlan, F. and Lam, S.S. (2015). Supply chain risk modelling and mitigation. *International Journal of Production Research* 53(18), 5640–5656.
19. Davarzani, H., Zanjirani Farahani, R., and Rahmandad, H. (2015). Understanding econo-political risks: Impact of sanctions on an automotive supply chain. *International Journal of Operations & Production Management* 35(11), 1567–1591.
20. Ceryno, P.S., Scavarda, L.F., and Klingebiel, K. (2015). Supply chain risk: Empirical research in the automotive industry. *Journal of Risk Research* 18(9), 1145–1164.
21. Trkman, P., de Oliveira, M.P.V. and McCormack, K. (2016). Valuie-oriented supply chain risk management: You get what you expect. *Industrial Management & Data Systems* 116(5), 1061–1083.
22. Burdeen, F., Shuaib, M., Wijekoon, K., Brown, A., Faulkner, W., Amundson, J., Jawahir, I.S., Goldsby, T.J., Iyengar, D. and Boden, B. (2014). Quantitative modeling and analysis of supply chain risks using Bayesian theory. *Journal of Manufacturing Technology Management* 631–654.
23. Elleuch, H., Hachicha, W., and Chabchoub, H. (2014). A combined approach for supply chain risk management: Description and application to a real hospital pharmaceutical case study. *Journal of Risk Research* 17(5), 641–663.
24. Colicchia, C., Dallari, F., and Melacini, M. (2011). A simulatin-based framework to evaluate strategies for managing global inbound supply risk. *International Journal of Logistics: Research & Applications* 14(6), 371–384.
25. Swenseth, S.R. and Olson, D.L. (2014). Simulation model of professional service personnel inventory. *International Journal of Services and Operations Management* 19(4), 451–467.
26. Ghadge, A., Dani, S., Chester, M. and Kalawsky, R. (2013). A systems approach for modelling supply chain risk. *Supply Chain Management* 18(5), 523–538.
27. Wangphanich, P., Kara, S. and Kayis, B. (2010). Analysis of the bullwhip effect in multi-product, multi-stage supply chain systems – a simulation approach. *International Journal of Production Research* 48(15), 4501–4517.
28. Wu, D. and Olson, D.L. (2011). Forward. *Annals of Operations Research* 185 (1), 1–3; Wu, D.D., Olson, D.L. and Birge, J. (2011) Guest editorial. *Computers and Operations Research* 39(4), 751–752; Wu, D., Olson, D.L. and Birge,

J. Introduction to special issue on enterprise risk management in operations. *International Journal of Production Economics* 134(1); Wu, D., Fang, S.-C., Olson, D.L. and Birge, J.R. (2012) Introduction to the special issue on optimizing risk management in services. *Optimization* 61(10–12), 1175–1177; Wu, D.D. and Olson, D.L. (2013) Computational simulation and risk analysis: An introduction of state of the art research.*Mathematical & Computer Modelling* 58, 1581–1587; Wu, D.D., Chen, S.-H. and Olson, D.L. (2014) Business intelligence in risk management: Some recent progresses. *Information Sciences* 256(20), 1–7.

29. Aqlan, F. and Lam, S.S. (2015). Supply chain risk modelling and mitigation. *International Journal of Production Research* 53(18), 5640–5656.
30. Ting, S.L., Tse, Y.K., Ho, G.T.S., Chung, S.H. and Pang, G. (2014). Mining logistics data to assure the quality in a sustainable food supply chain: A case in the red wine industry. *International Journal of Production Economics* 152, 200–209.
31. Cucchiella, F. and Gastaldi, M. (2006). Risk management in supply chain: A real option approach, *Journal of Manufacturing Technology Management* 17:6, 700–720.
32. Chopra, S. and Sodhi, M.S. (2004). Managing risk to avoid supply-chain breakdown, *MIT Sloan Management Review* 46:1, 53–61.
33. Wu, T., Blackhurst, J. and Chidambaram, V. (2006). A model for inbound supply risk analysis. *Computers in Industry* 57, 350–365. et al. (2006), op cit.
34. Cucchiella and Gastaldi (2006), op cit.
35. Blackhurst, J.V., Scheibe, K.P. and Johnson, D.J. (2008). Supplier risk assessment and monitoring for the automotive industry. *International Journal of Physical Distribution & Logistics Management* 38:2, 143–165.
36. Manuj, I. and Mentzer, J.T. (2008). Global supply chain risk management, *Journal of Business Logistics* 29:1, 133–155.
37. Wagner, S.M. and Bode, C. (2008). An empirical examination of supply chain performance along several dimensions of risk, *Journal of Business Logistics* 29:1, 307–325.
38. Lavastre, O., Gunasekaran, A. and Spalanzani, A. (2014). Effect of firm characteristics, supplier relationships and techniques used on supply chain risk management (SCRM): An empirical investigation on French industrial firms. *International Journal of Production Research* 52(11), 3381–3403.
39. Cucchiella and Gastaldi (2006), op cit.
40. Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.-M. and Tuominen, M. (2004). Risk management processes in supplier networks, *International Journal of Production Economics* 90:1, 47–58; Khan and Burnes (2007), op cit.; Autry, C.W. and Bobbitt, L.M. (2008). Supply chain security orientation: Conceptual development and a proposed framework, *International Journal of Logistics Management* 19:1, 42–64; Manuj and Mentzer (2008), op cit.
41. Kleindorfer and Saad (2005), op cit.
42. Chopra and Sodhi (2004), op cit.

43. Kahn, O. and Burnes, B. (2007). Risk and supply chain management: Creating a research agenda. *International Journal of Logistics Management* 18(2): 197–216.
44. Wagner and Bodhi (2008), op cit.
45. Manuj and Mentzer (2008), op cit.
46. Oke, A., Gopalakrishnan, M. 2009. Managing Disruptions in Supply Chains: A Case Study of a Retail Supply Chain. *International Journal of Production Economics* 118(1); 168–174.
47. Chopra and Sodhi (2004), op cit.
48. Talluri, S., Kull, T.J., Yildiz, H. and Yoon, J. (2013) Assessing the efficiency of risk mitigation strategies in supply chains. *Journal of Business Logistics* 34(4), 253–269.
49. Tang, C.S. (2006). Robust strategies for mitigating supply chain disruptions, *International Journal of Logistics: Research and Applications* 9:1, 33–45.
50. Cucchiella and Gastaldi (2006), op cit.
51. Ritchie and Brindley (2007a), op cit.