PRODUCTION AND OPERATIONS MANAGEMENT

POMS

Vol. 14, No. 1, Spring 2005, pp. 53–68
ISSN 1059-1478 | 05 | 1401 | 053$1.25

Managing Disruption Risks in Supply Chains

Paul R. Kleindorfer • Germaine H. Saad
Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania 19104, USA
School of Business Administration, Widener University, One University Place, Chester, Pennsylvania 19013, USA
kleindorfer@wharton.upenn.edu • germaine.h.saad@widener.edu

There are two broad categories of risk affecting supply chain design and management: (1) risks arising from the problems of coordinating supply and demand, and (2) risks arising from disruptions to normal activities. This paper is concerned with the second category of risks, which may arise from natural disasters, from strikes and economic disruptions, and from acts of purposeful agents, including terrorists. The paper provides a conceptual framework that reflects the joint activities of risk assessment and risk mitigation that are fundamental to disruption risk management in supply chains. We then consider empirical results from a rich data set covering the period 1995–2000 on accidents in the U.S. Chemical Industry. Based on these results and other literature, we discuss the implications for the design of management systems intended to cope with supply chain disruption risks.

Key words: disruptive risks; operational risks; supply chain management
Submissions and Acceptance: Received December 2003; revision received June 2004; accepted December 2004.

1. Introduction

This paper introduces a conceptual framework and initial results for the emerging area of disruption risk management in supply chains. The framework proposed builds on the risk management literature and models of supply chain coordination. The key issue addressed is the effect of alternative supply chain design options on the efficiency and robustness of the supply chain to various sources of disruption. We distinguish such disruption risks from normal supply-demand coordination risks. The latter issue has been the focus of a great deal of activity in the supply chain management literature in general (e.g., Fisher et al. 1997; Fine 2000; Levi et al. 2001; Lee 2002; Saad 2003; Balakrishnan and Geunes 2004; Boyaci and Gallego 2004; Souza et al. 2004; Gan et al. 2004, 2005)); and the literature on supply chain contracting in particular (e.g., Kleindorfer and Wu 2003; Cachon 2003; Kraiselburd et al. 2004; Gerchak and Wang 2004; and Martinez-de-Albeniz and Simchi-Levi 2005). This literature has been mainly concerned with on-going volume and earnings risks associated with coordinating demand and supply of multiple supply chain actors.

Disruption risk management, the focus of this paper, includes: operational risks (equipment malfunctions, unforeseen discontinuities in supply, human-centered issues from strikes to fraud), and risks arising from natural hazards, terrorism, and political instability. Disruption risk has received increasing attention in the last few years. The reason is undoubtedly that, with longer paths and shorter clock speeds, there are more opportunities for disruption and a smaller margin for error if a disruption takes place. The Taiwan earthquake of September 1999, which sent shock waves through the global semiconductor market (Papadakis and Ziemba 2001), the terrorist attack on the World Trade Center on September 11, 2001, and the August 14, 2003 blackout in the Northeastern U.S. are but a few recent reminders of the potential for significant disruptions to supply chains. Hendricks and Singhal (2003, 2005) analyze announced shipping delays and other supply chain disruptions reported in the *Wall Street Journal* during the 1990s and show, based on matched sample comparisons, that companies experiencing such disruptions under-perform their peers significantly in stock performance as well as in operating performance as reflected in costs, sales, and profits. As reported in Kleindorfer et al. (2003), disruptions from accidents in the chemical industry have led to huge economic losses and environmental damages, from the Bhopal and Exxon Valdez disasters, to the hundreds of lesser events that continue to occur on a yearly basis. These results add substance to the generally held intuition that supply chain disruptions should be a high priority topic for senior management and shareholders.

Our approach in addressing the question of effectively managing disruption risks faced in supply chain operations seeks to achieve two goals:

1. Develop a conceptual framework that reflects the effective integration of the joint activities of risk assessment and risk mitigation.
2. Provide strategic directions, actions, and necessary conditions that help advance cost-effective mitigation practices.

Our approach is based in part on empirical results from the U.S. Chemical industry, and a synthesis of pertinent concepts drawn from several literatures, including: risk management (Haimes 1998); industrial ecology and process safety (Kleindorfer 2001); supply chain management (e.g., Chopra and Meindl 2004; Kleindorfer and Van Wassenhove 2004); and quality management (e.g., Saad et al. 2000); as well as general principles from finance, engineering, and operations.

Our framework is based on four main premises, derived from the theory and practice of industrial risk management (e.g., Haimes 1998). *First*, is that in order to manage risk, one has to specify the nature of the underlying hazard giving rise to this risk. *Second*, the risk has to be quantified through a disciplined risk assessment process. This includes determining the pathways by which such risks may be triggered. *Third*, to effectively manage risk, the approach used must fit the characteristics and needs of the decision environment. Hence, the dynamics and needs of different supply chain environments will give rise to differences in approaches to assessment and design. *Fourth*, appropriate management policies and actions need to be integrated with on-going risk assessment and coordination among supply chain partners. These four premises comprise three main tasks that have to be practiced continuously and concurrently as the foundation of disruption risk management. The three tasks are: **S**pecifying sources of risk and vulnerabilities, **A**ssessment, and **M**itigation which we denote as (SAM).

The plan of this paper will follow the SAM framework. Section 2 makes use of the above premises for supply chain disruption management, and provides a set of principles for guiding the concurrent practice of the three SAM tasks involved. Section 3 presents a conceptual framework for risk analysis, which is supported by empirical evidence from the U.S. Chemical Industry, on the factors that appear to characterize risk management of disruptions in this industry. Building on this, we discuss the likely evolution of management systems that address disruption risk management, including security threats, arguing that these systems will take a form similar to the evolution of the ISO 9000 management system standard for quality. We conclude in Section 4 with a discussion of the implications of our analysis and empirical findings for emerging best practices in managing supply chain disruption risks. This includes proposed directions, actions, and necessary conditions for effective implementation in practice.

2. Managing Disruption Risk: Theory and Practice

Let us consider the SAM tasks introduced above in more detail.

2.1. Specify Risk Sources and Vulnerabilities (S)

Disruption risk may arise from many different sources:

2.1.1. Operational Contingencies. These include equipment malfunctions and systemic failures, e.g., the August 14, 2003 grid blackout in the northeast region of the United States. Other important contingencies include abrupt discontinuity of supply, for instance when a main supplier goes out of business; bankruptcy and other less severe forms of financial distress; and human-centered issues ranging from strikes to fraud.

2.1.2. Natural Hazards Earthquakes, Hurricanes, and Storms. For instance, the recent Florida series of hurricanes in 2004, Hurricane Andrew in 1992, and the Kobe earthquake in Japan in 1995 caused huge shipping disruptions in Florida and the Far East, and large losses to industry. The event study by Papadakis and Ziemba (2001) traces the financial consequences of the Taiwan earthquake in September 1999 for alternative supply chain models (build-to-order versus build-to-stock) and shows the shock waves that this event caused for global semiconductor markets.

2.1.3. Terrorism and Political Instability. The most salient event here is certainly the 9/11/2001 World Trade Center attack, but sabotage and destructive competitive acts, and political instability in different countries at different periods have clearly increased around the world, and these are increasingly affecting supply chains because of the increase in global outsourcing and the attendant increased length and complexity of supply chains (see Robb and Bailey 2003; Kleindorfer and Van Wassenhove 2004).

Supply chain strategies available to address these disruption risk vulnerabilities are focused on three areas: (1) the design of the product supported by the supply chain; (2) the supply chain itself, including location of inventories, transportation modes, and sourcing arrangements; (3) the operational control of the supply chain, including emergency (or crisis) response. For each of these three decision/design issues, a gated screening process implements the classical risk management paradigm (Haimes 1998) of identifying vulnerabilities, assessing their consequences, and mitigating risks that are deemed unacceptable. Sources of disruption risk relating to these areas include both materials in the product as well as execution modes for the supply chain itself. The key questions addressed in risk management are: what are potential sources of major disruption, and how can these be avoided or mitigated?

2.2. Risk Assessment (A) and Mitigation (M)

The methodology employed in industry, from financial services to the process industries, is based on three main disciplines: probabilistic risk assessment using fault and event trees; vulnerability assessment using emerging team based approaches for purposeful agents; and decision analysis. These are implemented with simulation software and backed by judgmental assessments. In response to the new challenges of terrorism, where probabilistic assessment presents major difficulties, the use of worst case analysis and contingent response scenarios has developed (Grossi et al. 2005). In response to the same challenges, Business Continuity Planning is now recognized as an important strategic priority in designing and rehearsing the organizational and communications architecture for on-going disruption risk management and for crisis management and emergency response (Harrald 2002).

To implement the three SAM tasks introduced above, we formulate a set of 10 principles, derived from the industrial risk management and supply chain literatures, that we argue must be understood *collectively* and *simultaneously* implemented in an integrative and coherent way to guide practice. We state these first and then discuss the rationale for each of them.

(1) One has to put one's own house in order first before expecting or requiring others in the extended supply chain to do so.

(2) Make use of, and extend the main premise of portfolio theory, namely: *diversification* reduces risk. For disruption risk management, such diversification should be extended to include facility locations, sourcing options, logistics, and operational modes.

(3) Robustness to disruption risks in a supply chain is determined by the weakest link in the chain, especially with respect to the actions of purposeful agents attempting to disrupt supply operations.

(4) Prevention is better than cure, i.e., loss avoidance and preemption are better than mitigation of losses after the fact.

(5) Extreme leanness and efficiency may result in increasing the level of vulnerability, at both the individual firm level and across the supply chain.

(6) As a corollary to principle 5, establishing backup systems, contingency plans, and maintaining reasonable slack, can increase the level of readiness in managing risk.

(7) Collaborative sharing of information and best practices among supply chain partners is essential in identifying vulnerabilities and in preparing for and executing effective crisis management.

(8) Good crisis management is not enough; linking risk assessment and quantification with risk management options ex ante is of fundamental importance in understanding the potential for ultimate harm to the organization from supply chain disruptions and for evaluating and undertaking prudent mitigation.

(9) Modularity of process and product designs, and other key elements of agility and flexibility for lean supply chain design, can also provide leverage for risk reduction, especially for interruptions involving discontinuities in raw material availability and component supply.

(10) Applying TQM principles, e.g., the Six-Sigma Approach, provides leverage in achieving higher supply chain security and reduction of disruptive risks faced while reducing operating costs.

The first principle derives from the fact that a supply chain network consists of three main subsystems: Supplier Relationship Management (SRM), Internal Supply Chain Management (ISCM), and Customer Relationship Management (CRM), respectively (see, e.g., Monczka et al. 2002; Chopra and Meindl 2004). The ISCM is the core of any chain, as it links both the producer and supplier's network (SRM), on the one hand, and the producer and its customers/distribution network (CRM) on the other hand, Thus, internal supply chain integration and optimization must precede any inter-firm interfaces. In particular, site/facility management systems to identify and mitigate disruption risks are the central building blocks for supply chain-wide systems. This principle also implies that senior management commitment and oversight to the disruption risk management process is essential.

The second principle is an extension of portfolio theory in finance, where a fundamental result is that portfolio diversification reduces the investor's risk (see, e.g., Lasher 2003; Gallagher et al. 2000; among others). This theory is of particular relevance here as we extend its application to include diversification of facility locations, products and services produced, sourcing options used, as well as operating modes and processes; only with such multidimensional diversification can the full potential of risk minimization be reached.

The third principle implies that disruption risk management must attempt to provide incentive alignment and collaboration for risk avoidance and reduction among all supply chain partners. One weak partner in the supply chain can prove disastrous for all participants, especially when purposeful agents analyze rationally where to target their disruptive attacks. Depending on the product and supply chain characteristics, robustness and/or profitability will be strongly affected by the weakest link in the chain (e.g., Handfield and Nichols 2002; Baiman et al. 2003; Kunreuther and Heal 2004). This principle requires that vulnerabilities be identified across the entire supply chain, together with early warning and crisis management systems. Rehearsal and testing existing systems through periodic staged events is an important element of testing for both internal and extended supply chains.

The fourth principle implies that risk avoidance should precede risk reduction (Michaels 1996). This dominant relationship is reflected in both our conceptual development and action guidelines derived from existing practice (see Pauchant and Mitroff 1992). This principle implies that investments in risk assessment to determine key vulnerabilities, as well as worst case scenarios arising from such vulnerabilities, are a critical first-step in disruption risk management, and contingency plans for responding to worst case scenarios are of particular relevance in prioritizing mitigation strategies (e.g., Baird and Thomas 1985; Saad and Siha 2000). These schemes singularly and collectively help to understand and avoid risks in the first place, while increasing the level of readiness and preparedness to respond to risks that may endanger the mission of the firm itself.

The fifth principle implies that in order to minimize risk, and ultimately loss from supply chain disruptions, attention must be given to the tradeoff between "robustness" of the supply chain to disruptions and the overall efficiency of the supply chain under normal operations. While many writings in the last two decades have emphasized the importance of leanness in internal operations as well as in the extended enterprise, much less attention has been given to the trade-off between leanness on the one hand, and systems' reliability and supply chain robustness on the other hand. One consequence has been the significant increase in the number and costliness of supply chain disruptions as noted by Hendricks and Singhal (2003).

The sixth principle notes the traditional path to increased supply chain robustness, namely the use of reliability theory and process improvement (e.g., Upton 1996, pp. 3–19; Stevenson 2004, pp. 155–164)), including redundancy and appropriate back-up systems. It should be noted here that back-up systems can be made available in either physical form, virtual form, or both. Additional useful practice can be drawn here from the theory of organization design and dynamics, including healthy slack in production and operations planning, as espoused by Galbraith (1973, 1977) and "normal accident" theory developed by Perrow (1999).

The seventh principle implies that cooperation, coordination, and collaboration have to prevail both cross-functionally within the firm, and across supply chain partners. Non-cooperative strategies in managing disruption risks are too costly, and leave synergies unexploited. Moreover, with an eye on the second principle, weak links cannot be identified and enhanced without such collaboration. Practitioners at all levels have to seek and achieve "win-win" outcome. Recognizing the importance of such behavioral themes, these are central aspects of the Supply Chain Operational Reference Model (SCOR) developed by the Supply Chain Council and is widely in use now nationally, and internationally. They are also evidence in industry-wide approaches to developing best practices for security and terrorism (Rice et al. 2003).

The eighth principle notes the outcome of several decades of progress in risk management and insurance (Haimes 1998; Kunreuther et al. 2004). It captures the essential wisdom of Peter Drucker and many others to the effect that "You cannot manage what you do not measure." As Rice et al. (2003) note, quantification of risks is also essential to making the business case for mitigation. Without such quantification, there may be a general sense of alarm in the firm and the supply chain, but this will not be directed towards the most cost-effective means of mitigating expected and worst case scenarios until risk assessment and risk management of supply chain disruption risks are undertaken using probabilistic risk assessments, and practices implemented are properly audited for compliance. Using preemptive/alerting triggers, as near miss systems (see, e.g., Phimister et al. (2003), and defect prevention schemes from quality management (Chase et al. (2004), measurement of weak points in supply chain and facility operations can be embedded in on-going process management.

The ninth principle emphasizes flexibility and mobility of resources to reduce risk and increase the speed of response to contingencies. This has been understood for some time in international supply chain design (e.g., Huchzermeier and Cohen 1996; Lee 2002) as a means of operationally hedging such risks as currency risks and volatility in local input prices and regional demand. It is now recognized more generally that such mobility and flexibility promotes resilience in the supply chain better when resources and essential inputs are fungible, as they are under modular design, delayed differentiation, and other elements of modern supply chain design. In this sense, resilient supply chains are not inimical to efficiency and lean operations, but the dimensions of resilience and robustness to supply chain disruptions must be explicitly considered in the design process if they are to be captured (Rice et al. 2003).

The tenth principle reflects the fact that making use of TQM tools in general, and the six sigma approach in particular results in reducing disruption risks faced in supply chains. Such use not only enhances supply chain security, especially for international cargo shipments by sea, but simultaneously reduces operating costs. Recent information coding systems and the use of RFID (radio frequency identification) technology have made such achievements now a reality. More details on how to increase supply chain security while reducing operating costs using TQM tools has been recently reported by Lee et al. (2003a, 2003b).

The theory of disruption risk management builds on work of Holmstrom (1982) and others who have analyzed the incentives that various parties in a multi-agent setting face to undertake effort that will benefit the entire group of agents. In the area of risk, the simplest useful framework derives from the work of Shavell (1984), and we will use it to motivate our empirical work in the next section. We suppose a company is interested in the tradeoff between the cost of risk mitigation investments, including the cost of management systems, and the expected costs of disruptions. We imagine, at most, one disruption can occur during a planning period and represent the total costs of investment and disruption as:

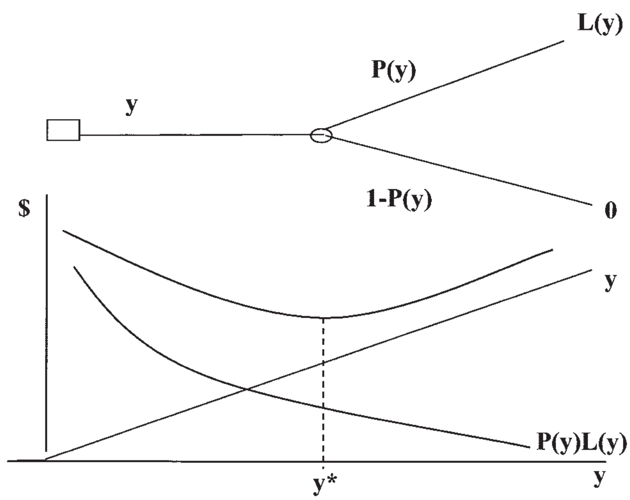
$$\text{Expected Costs} = y + P(y)L(y)$$

where:

y = $ Investment to Mitigate Probability of Disruption or Resulting Loss

y* = Optimal Investment Level on Mitigation Activity

Figure 1 Simple Framework for Risk Mitigation from Shavell (1984).



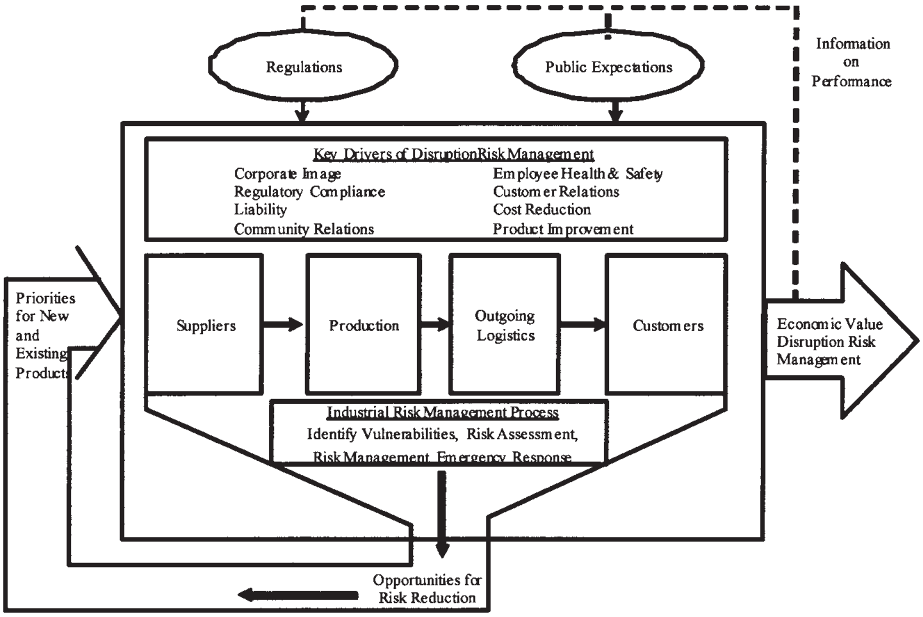
P(y) = Probability of a Disruption during Time Frame of Interest, a function of y

L(y) = $ Amount of Loss as a function of y

To minimize total costs, the trade off is between the investment in mitigation (y) and the disruption loss L(y), weighted by the probability of a disruption. The optimal level y*, is where the total costs are minimum as illustrated in Figure 1. This framework captures one essential element of the risk management process, mitigation. The other essential element is the cost of acquiring reliable information on P(y) and L(y). This is the risk assessment process. To be effective, risk mitigation must be preceded by, and based on, an informative risk assessment process. We will not pursue here the standard decision analytic problem of determining the jointly optimal investment levels in information acquisition and mitigation (see Hertz and Thomas 1984). These follow the classic Bayesian value of information framework. It should be evident, however, for both single-company and multi-company supply chains, that there are tradeoffs between the cost of acquiring reliable information on risks and the ensuing mitigation activities. At optimum, a balance must be struck between the marginal costs and benefits of better risk assessment (assuring the quality of risk information) and the marginal costs and benefits of the optimal mitigation that must be chosen, conditional on the level of risk information yielded by the risk assessment process.

In the multi-company supply chain, two key issues arise: first, is the requirement in the risk assessment process to have supply-chain wide visibility of vulnerabilities; second, is to establish appropriate incentives across participants in the supply chain to identify and implement disruption management systems. The first of these requires information sharing across supply chain participants, and is certainly not an easy matter, since a company with special vulnerabilities may have every incentive to hide these from other supply chain participants. The second is even more difficult since it may entail significant resource commitments, and sharing the costs and benefits of these through pricing, business continuing insurance and other available supply chain contracting instruments is non-trivial (Baiman et al. 2003). We note that current communication and information technologies, e.g., using compatible ERP systems and CPFR (Collaborative Planning, Forecasting and Replenishment) methods, allow for improved integration of information flows and supply chain visibility among all participants, or actors in the chain (Chopra and Meindl 2004; Stevenson 2004). But vulnerabilities to disruption are, by their very nature, more difficult to identify. What is needed is for the overall supply chain risk to be properly signaled to each participant, so that, at the least, investments that make sense to individual companies

Figure 2 Risk Analysis and the Extended Supply Chain.



are not omitted. At this stage of development in the practice of supply-chain wide disruption risk management, the primary vehicle for coordinating disruption risk management across multi-company supply chains is non-performance penalties built into contracts (Baiman et al. 2003). It is not clear, even in theory, whether such penalties can be properly structured to achieve an efficient outcome. Beyond improving visibility on supply chain vulnerabilities and associated information sharing on risk mitigation among supply-chain participants, creating appropriate contracting options and incentives for improvements in disruption management remains an art form, with a host of open theoretical and empirical research questions to which we return below.

The business process for accomplishing risk reduction consists of overlaying the new product development process and supporting supply chain design with a series of screens, which subject new products and processes to a detailed assessment according to an established protocol. As shown in Figure 2 (from Kleindorfer 2001), the disruption risk management process then acts as a "funnel" to discover and quantify hazards in the extended supply chain and to mitigate those for which cost-effective risk reduction measures are feasible. One phased approach to disruption risk management that has been developed with industry at the Wharton Risk Center over the past decade includes the following four steps:

1. Obtain senior management understanding and approval, and set up organizational responsibilities for managing the Disruption Risk Management process. This activity is frequently linked to other forms of risk management and increasingly to enterprise-wide risk management (see Buehler and Pritsch 2003).

2. Identify key processes that are likely to be affected by disruptions and characterize the facilities, assets, and human populations that may be affected. Key processes typically include new product development, supply chain operations, and manufacturing. Key assets include both tangible assets (property and inventory) as well as intangible assets (brand image, public perceptions).

3. Traditional risk management is then undertaken for each key process to identify vulnerabilities, triggers for these vulnerabilities, likelihood of occurrence, and mitigation and risk transfer activities. This is the heart of the traditional industrial risk management process for disruption risks. This activity gives rise to two important outcomes: first, is a taxonomy of major disruption risk categories that confront key assets of the firm; second, are the management systems that implement a company's approach to risk management and ensure the integration of risk management activities with other management systems (quality, production, maintenance, environmental, health and safety, and so forth).

4. Reporting, periodic auditing, management, and legal reviews of implementation plans and on-going results (e.g., of near-miss management and other disruption risks) complete the business process for disruption risk management. The audit process, whether undertaken by the firm, by second parties (contracted by the firm), or by third-parties (external certified examiners), is essential to providing on-going feedback to management and supply chain participants on

the performance of their facilities and their compliance with agreed, supply-chain wide standards.

For accidental triggers, benchmarking (both internal and external), and industry or sectoral studies can provide an on-going basis for understanding the sources of major disruption. For purposeful triggers, including terrorist acts, a process that has been known in the military for some time is useful, that of role-playing or "red-blue teaming". Under this approach, supply chain experts, equipped with whatever information is available, attempt to "attack" the supply chain to cause major disruptions. The Red Team in this exercise generates a set of scenarios that they believe can lead to serious disruptions. The Blue Team attempts to provide mitigation or countermeasures that are cost effective against the Red Team scenarios. A multi-level exercise at each link of the supply chain directed towards uncovering significant vulnerabilities can be very effective both in understanding the vulnerabilities of a supply chain to disruptions as well as in making members of the risk management team aware of what can be done to either mitigate these or at least to be prepared to respond to them.

The use of external, industry-wide benchmarks for identifying sources of disruption risk is illustrated in the next section where we report recent results from the accident history data reported under 112(r) of the Clean Air Act Amendments. A great deal of knowledge exists in specific sectors (e.g., the chemical sector, the petroleum sector, and retailing) on operational and technical approaches to disruption risk management, including environmental, health and safety management systems, automated diagnostics, and a host of other detection, preparedness, and prevention technologies. While such sector-specific knowledge is extremely important in providing on-going guidance in this area, it is also important for the general development of the field to continue to search for generalizable approaches to disruption management and the theory that guides these.

3. Experience from the U.S. Chemical Industry

The tragedy at Bhopal in December 1984, followed by a subsequent release of aldicarboxime from a facility in Institute, West Virginia resulted in great public concern in the United States about the potential danger posed by major chemical accidents. This public concern was translated into law in section 112(r) of the 1990 Clean Air Act Amendments. Section 112(r) sets forth a series of requirements aimed at preventing and minimizing the consequences associated with accidental chemical releases. These requirements reflects several of the principles stated in Section 2 above, in particular, the first, the fourth, and the eighth principles, and are the basis of EPA's rule on "Risk Management Programs for Chemical Accidental Release Prevention" (hereafter the "RMP Rule"). The RMP Rule is important for understanding supply chain disruption risks since it contains a fairly complete record of accident activity for an important industrial sector during the 1995–2000 time frame, whether these accidents resulted from natural hazards, equipment or human failure, or sabotage. Here, we report some results from the data and then explore some of the practices triggered by this data for disruption risk management. This data is at the facility level, and not at the supply chain level, but this is clearly important for supply chain management, as production and warehousing facilities are the key building blocks of supply chains. But this data will miss transportation disruptions that occur en route.

With some exceptions, the implementation of 112(r) in an EPA regulation (which bears the official regulation number of "40 CFR 68"), required all facilities (public and private) storing on-site any of 77 toxic or 63 flammable substances above specified threshold quantities to prepare and execute a Risk Management Program (RMP), which contains the following elements:

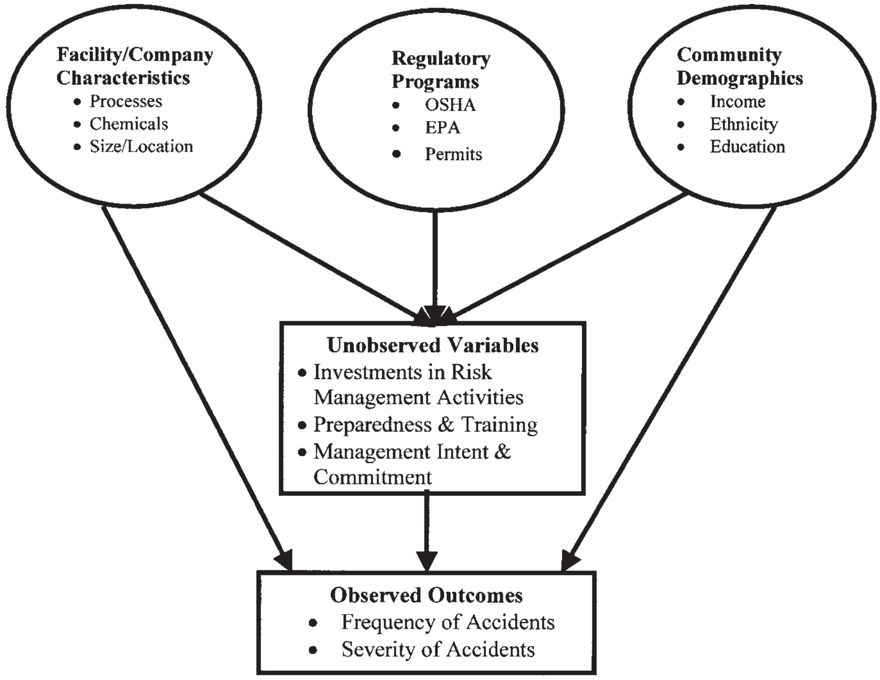
1. A Risk Management Plan, a report capturing certain details about the facility's accident prevention program, emergency response program, and hazard assessment along with administrative information about the facility.
2. A hazard assessment to determine the consequences of a specified worst-case scenario and other accidental release scenarios on public and environmental receptors and provide a summary of the facility's five-year history of accidental releases.
3. An accidental release prevention program designed to detect, prevent, and minimize accidental releases.
4. An emergency response program designed to protect human health and the environment in the event of an accidental release.

By December of 2000, the cutoff date for the analysis that follows, a total of 15,219 facilities reported to this database. All facilities were to report accidental releases of covered chemicals or processes that resulted in deaths, injuries, significant property damage, evacuations, sheltering in place, or environmental damage (see Kleindorfer et al. (2003) for details).

Figure 3 shows the data elements available in the RMP database, or those obtainable from other collateral databases (e.g., census data matched to the facility location). The following hypotheses arise naturally from this figure concerning the frequency and severity of disruptions:

1. The characteristics of the facility itself will have a significant impact on the frequency and severity of

Figure 3 Framework of Analysis for Chemical Industry.



disruptions at the facility. Characteristics of importance include facility location, size, and the type of hazard present; as well as characteristics of the parent company/owner of the facility (capital structure, sales, etc.)

2. The nature of regulations that a facility faces and the nature of enforcement activities associated with these regulations will be significantly associated with observed frequency and severity of disruptions at the facility.

3. The socio-demographic characteristics of the host community for the facility will affect the level of pressure brought on the facility to operate safely and to inform the community of the hazards it faces, and this pressure in turn will be negatively associated with the frequency and severity of disruptions at the facility.

It is important to note the role of the unobserved managerial factors noted in Figure 3 on observed outcomes. These managerial factors may be fundamental drivers of the accident propensity and preparedness of facilities, but they are confounded with these outcomes. For example, the direction of the statistical association between more stringent regulatory structures and accident rates is not clear ex ante. On the one hand, more stringent regulations might serve to promote better risk assessment procedures, leading to more effective risk mitigation expenditures and reduced accident rates (following the simple Shavell Model captured in Figure 1). However, more hazardous facilities are likely to be the focus of more stringent regulations, and the greater hazard of these facilities may more than counterbalance the impact of the regulation. The same confounding of the unobserved effects could be elaborated for the other predictors and outcomes in Figure 3. Thus, in general, the statistical associations identified here will reflect the combined effects of regulatory oversight, community pressure, and facility characteristics, as these interact with owner/shareholder governance and management systems put in place to monitor and control facility activities. It is therefore an empirical question to determine how company management is actually responding to the dictates of specific management-based regulations like the RMP Rule.

Let us first consider the association between facility characteristics and regulatory programs with a facility's accident history. The facility characteristics that we consider are the following: geographic region; size of facility; and chemicals used at facility. The quantity and nature of chemicals used at each facility are summarized for our statistical analyses by a single "total hazard measure," defined roughly as a measure of the hazard of the chemicals on site and the number of covered processes at the facility. More precisely, the *total hazard* measure used is defined as the sum over all chemicals of $\log_2$(maximum quantity of inventory on site/threshold), or, alternatively, as the number of chemicals times $\log_2$ of the geometric mean of the maximum-to-threshold quantity ratio. Hence a total hazard measure of 0 indicates that only threshold levels of chemicals are kept in inventory, a measure of 1 means 1 chemical is kept at up to twice threshold level, 2 means 2 chemicals kept at up to twice threshold level or 1 chemical at up to 4 times threshold level, and so forth; unit changes in this measure can thus be interpreted as either an doubling of volume inventoried of a single chemical or an addition of another twice-threshold chemical on-site.

The regulatory programs studied are OSHA-PSM (the process safety management standard overseen by OSHA); CAA Title V (the air quality and permitting standard, applicable to facilities that have the potential to release airborne toxics); and EPCRA-302 (the Emergency Planning and Community Right to Know Act that specifies for regulated facilities the information that they must make available to the public).

Standard logistic regression models termed proportional odds (PO) models (Agresti 2002) are typically used to estimate the relative change in odds of a facility being at level j rather than $j - 1$ for a unit change in a covariate. Here, we use a two-level ordinal scale, with $j = 0$ being no accidents, and $j = 1$ being one or more accidents. Confidence intervals for odds ratios are obtained via profile likelihood (Agresti 2002).

A total of 1,945 chemical-release accidents between 1995 and 1999 were reported among the 15,219 facilities, resulting in 1,973 worker injuries and $1,018,000,000 in on-site property damage (with business interruption and other indirect costs of such accidents unmeasured, but considered by industry specialists to be on the order of 3 to 10 times larger than the direct property damages measured). A total of 1,186 facilities (7.8%) reported at least one accident (range: 1–15). Of these accidents, 670 (4.3%) involved worker injuries (range: 1–69); and 316 (2.0%) involved facility property damage (range: $10–$219,000,000). Table 1 reports the facility, hazard, and regulatory variables of interest.

Table 2 shows, for facilities with at least one reported accident, Spearman correlations between characteristics of the facility and three outcome variables: number of accidents, number of injuries, and property damage. We note that facilities with more full-time employees, more hazardous chemicals in use, and greater total hazard measure were at greater risk of accident, worker injury, and property damage. There are regional differences among facilities, as well as expected differences in the results of toxics and flammables. Toxic chemicals were more strongly associated with worker injury, whereas flammables were more strongly associated with property damage, which makes sense because fire is obviously capable of causing a much greater degree of damage to property than release of acids or poisonous gases, which are either more contained or less damaging to property.

On the regulatory side, facilities regulated under the Right-to-Know Act (EPCRA-302) had a modestly higher risk of accident, injury, and property damage

Table 1 Characteristics of RMP Reporting Facilities, Overall and by Whether or Not an Accident was Reported in RMP (1995–1999)

	All facilities (n = 15,219)	No accident (n = 14,033)	1/+ accidents (n = 1,186)
Geographic region§**			
% Region I	1.5	1.5	1.7
% Region II	3.2	3.1	3.8
% Region III	5.6	5.4	8.0
% Region IV	15.7	15.5	18.8
% Region V	21.4	21.5	19.5
% Region VI	15.8	15.3	22.0
% Region VII	18.6	19.4	10.3
% Region VIII	6.6	6.8	4.1
% Region IX	8.2	8.3	7.8
% Region X	3.4	3.3	4.2
Number of Full-Time Equivalent Employees (FTEs)**	155	139	345
Number of Chemicals			
Toxic**	1.07	1.04	1.56
Flammable**	.30	.26	.79
All covered chemicals**	1.37	1.30	2.35
Total Hazard**†	13.8	12.7	26.6
% EPCRA-302**	82.2	81.9	85.9
% OSHA_PSM**	49.2	46.6	79.2
% CAA Title V**	14.6	13.2	31.9

* = $p < .05$, ** = $p < .01$ by Pearson chi-square or Wilcoxon rank test.
† Methodology for calculating "total hazard" is defined in the text above.
§ = EPA-defined geographic region; Region I: Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut; Region II: New York, New Jersey, Puerto Rico, Virgin Islands; Region III: Pennsylvania, Delaware, District of Columbia, Maryland, West Virginia, Virginia; Region IV: North Carolina, South Carolina, Georgia, Florida, Alabama, Mississippi, Tennessee, Kentucky; Region V: Ohio, Indiana, Michigan, Illinois, Wisconsin, Minnesota; Region VI: Arkansas, Louisiana, Texas, Oklahoma, New Mexico; Region VII: Missouri, Iowa, Nebraska, Kansas; Region VIII: North Dakota, South Dakota, Montana, Wyoming, Utah, Colorado; Region IX: Arizona, Nevada, California, Hawaii, Guam, American Samoa, Trust Territories, Northern Mariana Islands; Region X: Idaho, Oregon, Washington, Alaska.

than other RMP facilities, while facilities regulated under OSHA Process Safety Management and CAA Title V (regulating air pollution standards) had a much higher risk (see Table 3 below). Using a two-level logistics regression, we see from Table 4 that nearly all of this excess risk for Right-to-Know and CAA Title V facilities could be explained by their larger size and greater total hazard measures, whereas only about one-half of the excess risk for OSHA-PSM facilities could be explained in this manner. This makes sense in that EPCRA-302 and CAA Title V targets facilities with hazards having significant off-site consequences, while the OSHA-PSM standard is focused on on-site hazards, which may not be directly related to inventory levels or numbers of processes, as captured in our simple hazardousness measure.

Let us now briefly consider two other hypotheses related to Figure 3, those concerned with the financial structure of the parent company, and those concerned with the impact of socio-demographic variables of the

Table 2 Spearman Correlations Between Number of Accidents, Number of Injuries, and Property Damage in RMP (1995–1999) and Characteristics of Facility, Among Facilities (n = 1,186) With At Least One Accident

	Number of accidents	Number of injuries	Property damage
Number of FTEs	.23**	.20**	.14**
Number of chemicals			
Toxic	.15**	.13**	.04**
Flammable	.10**	.08**	.13**
All covered chemicals	.20**	.17**	.13**
Total Hazard	.13**	.12**	.10**

* = $p < .05$; ** = $p < .01$.

Table 4 Odds Ratios (ORs) For Having Any Versus No Accidents; Any Versus No Worker Injuries; and Any Versus No Facility Property Damage in 1995–1999, By Regulatory Oversight, Adjusted For Number of Full-Time Employees and Total Hazard Measure*

	Accidents	Injuries	Property damage
EPCRA-302 (vs. no)	1.15 (0.96–1.37)	1.33 (1.03–1.70)	0.94 (0.67–1.32)
OSHA_PSM (vs. no)	1.81 (1.53–2.16)	1.66 (1.31–2.11)	3.06 (2.03–4.61)
CAA Title V (vs. no)	0.90 (0.11–7.14)	0.91 (0.11–7.31)	1.22 (0.15–9.77)

* 95% Confidence Levels in Parentheses.

surrounding community in which facilities are located.

In Kleindorfer et al. (2004), we analyze the impact of parent company financial structure by considering a subset of the RMP data, namely the data for facilities whose parent company was publicly traded. This corresponded to 2,023 facilities (out of the original RMP database of 15,219 facilities). A number of financial variables are considered in Kleindorfer et al. (2004), but we will summarize the results here only for previous year debt/equity (D/E) ratio and total (net) sales, where debt-equity ratio was determined as the ratio of the long-term debt to the common equity.

The basic results for D/E ratio and Sales can be summarized as follows. After adjusting for the employment of facilities (the FTEs at the facility) and the average hazardousness of the facility (using the same "total hazard" measure as that underlying the tables above), Kleindorfer et al. (2004) find that: Parent company D/E ratio (respectively, Sales) has a significant positive (respectively, negative) association with accident and injury rates in the sample. We note that these results are in the direction that both intuition and theory would support. Companies that are more debt-ridden are likely to be less concerned with long-term cash flows, as most of the risk is borne by creditors who are not represented in the company's decision making about risk mitigating investments. Similarly, companies with large sales have a great deal at risk from disruptive accidents and this leads, as expected, to greater care and lower accident and injury rates. These results on capital structure of facility parent companies are therefore consistent with normal economic expectations.

Finally, concerning our hypothesis (see Figure 3) on community and demographic factors, there is an extensive body of research in political economics, public policy, and public health noting associations between environmental and health risks arising from industrial facilities and the socio-economic status (SES) of host communities. In brief, this would suggest the hypothesis that facilities located in lower-SES communities would see more hazardous facilities located there and would also see higher accident and injury rates resulting from such facilities. These associations could be caused by firms' preferring to locate hazardous facilities in lower-SES communities in which they anticipate lower levels of collective action and monitoring. These could also result from migration of groups of lower SES to sites where such facilities have located, since property values may be lower there. It is clearly of some interest to see if such socio-demographic effects are discernible in the RMP data.

This question has been studied in detail in Elliott et al. (2004). What Elliott et al. found for the RMP data is that higher accident and injury rates were associated with facilities located in counties with higher proportions of African-American population, even if they

Table 3 Mean Number of Full Time Employees (FTEs) and Total Hazard Measure, by Regulatory Status

	Regulated under					
	Right-to-know Act		Process safety mgmt		CAA title V	
	Yes	No	Yes	No	Yes	No
Mean FTEs	170	87	281**	34**	488**	99**
	(1291)	(332)	(1630)	(366)	(2191)	(886)
Mean total hazard§§	14.2**	12.2**	16.7**	11.1**	24.6**	12.0**
	(20.5)	(9.5)	(26.2)	(5.5)	(31.3)	(15.2)

* = $p < .05$, ** = $p < .01$ by Wilcoxon rank-test.
§§ = sum of $\log_2$ (maximum quantity of inventory on site/threshold).
Standard deviations are in parenthesis.

have the same amount of hazardous chemicals on site. The impact of income and poverty was, however, more complex. Larger facilities were more likely to be located in counties with higher median incomes and higher levels of income inequality, although part of this association is explained by the fact that larger facilities tend to also be located in counties with large populations and large manufacturing labor forces. Similarly, facilities in higher-income counties with higher levels of poverty, or at least without corresponding low poverty levels—again, high-income-inequality counties—were at greater operational risk as well. However, after adjusting for "total hazardousness", income and income inequality were no longer associated with operations risk. One explanation for these results is that communities burdened by low SES and past or present discrimination may be willing to accept these risks in order to obtain the economic benefits of facility location, or that residents not willing to accept this risk move away.

Taken together these results on the RMP data provide corroboration of the overall structure of Figure 3; each of the three factors displayed in Figure 3 appears to have associations as an independent driver of observed accident and injury rates. This suggests that both economic and social/legal factors play an important role in company strategy and that management systems, either voluntarily adopted, or triggered by risk and safety regulations such as the RMP Rule, for disruption risk management need to (and do) respond to a wide set of factors affecting individual companies and the supply chains they operate in. Thus, the issue of disruption risk management, at least in the chemical industry, extends well beyond the simple cost/benefit calculus captured in Figure 1. This is a theme we would now like to explore in more detail.

3.1. Implications of the RMP Data for Disruption Management Systems

The results of the initial analyses of the RMP data provide detailed characterizations of the statistical associations among facility characteristics, regulations and community demographics and accident rates and property damage. These are, for the most part, intuitive and support common wisdom in both the risk management community and the financial economics literature. Building on these results and the principles articulated earlier, one might posit the following hypotheses on the interaction of regulations to protect third parties (e.g., communities in the chemical context) and to tradeoff mitigation investments against reduced property and business losses. The RMP Rule, while specific to the chemical industry, is instructive as to the dynamic driving disruption risk management more generally. The RMP Rule itself has requirements for both changes in management systems (the development of a structure to manage risk assessment and risk mitigation and to report on the chemical risks involved), as well as information generation and sharing (in this case, accident history data, worst-case scenarios, and certain other elements of the Risk Management Program in the facility). These are expected to result in changes in management systems and, over time, in the codification, through consultants and auditors, of best practices. The informational requirements are expected to yield data that reveal characteristics about individual facilities as well as comparative baseline data for entire sectors and technologies. The improved information and standardization of management systems is expected to allow the identification of improvement opportunities as well as to focus the concerns and actions of stakeholders on what is important to them. Finally, this improved debate and the ability to carry out changes based on improved and dedicated management systems could lead to observed improvements in outcomes. Expected improvements range from more informed stakeholders, including management and employees of facilities, to improved risk-based pricing of insurance products, to the direct observable consequences of reduced frequency and severity of disruptions.

The general forces noted above have been observed in several other instances. We mention here only the ISO 9000 and ISO 14000 standards, the first for quality and the second for environmental systems. (See Kleindorfer 1997 and Corbett et al. 2002 for a more detailed discussion of these standards.) While these are voluntary standards, and not regulations, ISO 9000 is a requirement imposed by some governmental agencies on companies competing for public procurement contracts and some major customer groups (such as automotive) on their suppliers. The evolution of these standards follows essentially the logic noted above. Take ISO 9000. In the early 1990s when the standard first began to attract attention, because of a growing sense that contracting in the new European Union would make this a requirement, very little was known about the costs and benefits of ISO 9000. By the mid-90s, best practices in implementing the standard had been codified, and knowledge about these spread quickly around the world. Particular sectors, like the automotive sector, began to develop more refined versions of the standard for their sector. As standardization proceeded, best practices improved and researchers and practitioners were able to discern what worked and what didn't. After about a decade of experience, in many countries, it has become clear (see Corbett et al. 2002) that there is real payoff, in both financial and operational performance, from an appropriate implementation of ISO 9000. The magnitude of the payoff, including the costs of implementation, depends on the sector, the country of operations, and the experience of the implementing company with process management approaches to quality.

The same dynamic is also occurring with ISO 14000, but as it was just launched in 1996, it is not yet possible to discern the steady state outcomes from this standard. However, there is a growing expectation that ISO 14000 (and associated auditing standards) will have similar impacts in the environmental area to those achieved by ISO 9000 in the quality arena. Importantly, there are also what we call "synergies of excellence" arising from the joint application of ISO 9000 and ISO 14000. These synergies arise from the fact that both standards are process based and require a deep knowledge of operations at the process level. Accomplishing this pays dividends not just in terms of the focus of the standard (quality or environment), but also in more indirect ways in having employees involved in decision making, in establishing accountability and a culture of management by fact, and in many other ways noted by management scholars as important for operational and financial excellence. These synergies of excellence provide a strong additional, positive externality to improvements in management systems and information, and may also accompany management-based regulations, giving rise to unexpected additional benefits beyond those which were the original focus of the regulation.

Of course, "voluntary" quality and environmental standards may be quite different than management-based risk standards related to supply chain disruptions. Is there any reason to believe that we will see a similar evolution of the above dynamic in the disruption risk area? A good example of this is the current concern and activities associated with security of global supply chains.

In the aftermath of the 9/11 attacks, the Madrid train bombing, and the heightened concern about global terrorism, security of global supply chains and multi-modal logistics systems have become a focus of significant current activity in industry and government. A key objective is the determination of partnership principles that should guide the development of standards and certification procedures for global supply chains. For major retailers (like Wal-Mart and Home Depot) involved in container-based trade, a joint solution that assures continued facilitation of international trade with a high level of assured security is a must going forward. Major disruptions to any retailer from terrorist activities will have significant negative externalities for other retailers. Emerging principles underlying a public-private partnership approach to cargo security can be summarized as a "trusted supply chain partner program", in line with the provisions of C-TPAT (Customs-Trade Partnership against Terrorism). These principles have been further elaborated in the National Defense Transportation Agency (NDTA) Security Best Practices Committee, operating in cooperation with Department of Homeland Security and the Transportation Security Administration (DHS/TSA) (see also Rice et al. (2003)). The basic thrust of current activities is the development and diffusion of best practices in global supply chain security, including improved inspections and clearance processing in ports.

Under a standard like C-TPAT, global supply chains are expected be fully vetted for security, personnel, and process control. Supply chain compliance must also be fully auditable and integrated electronically with the appropriate Department of Homeland Security systems as well as those of relevant international customs agencies. The approach being pursued by global retailers is similar to that described above for the chemical sector. In particular, the approach foresees integrating the activities of the following key actors:

Private companies who manage global supply chains (including manufacturers at the front end and retailers and shippers downstream);

Port authorities and (de-) consolidators (in the U.S. and elsewhere) who have the responsibility for clearing cargo and for its loading/unloading;

Local, Regional and National agencies, including DHS/TSA who have the responsibility for assuring security at various levels, including responding to threats and abnormal conditions.

At the company level, the approach to disruption risk management encompasses security concerns from originating manufacturer to final retail outlets. The details of this approach are still evolving, but they are quite consistent with the SAM approach formulated in this paper. As in the ISO 9000 example noted above, the further evolution of these steps will likely follow a process similar to that mapped in Figure 4 below.

Large companies have already begun to develop security metrics (including the scope of integrity of seals, continuous movement of the container, length of time in exposed areas such as foreign ports, and a number of cost metrics) to evaluate approaches to improving global supply chain security. These approaches could profit greatly from the scenario-based Red-Teaming approach discussed above to discover and classify vulnerabilities, and to model the effects of disruptions. These vulnerabilities should be related to key elements of their global supply chain and to available methods and technologies for mitigation, including certification of personnel, audit procedures, and approaches to assuring the integrity (tamper-proofness) of containers. As in the chemical sector example, procedures must be developed to share the results of vulnerability analysis and related data with local, regional, and national response agencies. The key in the approach is to leverage those organizations in the

Figure 4 **Disruption Risk Management and Security in Global Supply Chains.**

• *Establish Voluntary Security Standard*	• *Classification of Assets/Processes*	• *Ranking & Prioritisation*	• *Iterate for Continuous Improvement*
1. Design a voluntary standard in Security Management that will allow private firms to achieve optimal "internal levels" of security • Compatible with current best industry practice • Coordinate with key private players to achieve "critical mass" to achieve tipping 2. Standard should define a process, along the lines of ISO 9000: • Management responsibility • Training • Documentation • Company-specific implementation	1. For each sector (shippers, consolidators, retailers, etc.) determine main assets/processes 2. Asses vulnerabilities of each asset/process jointly with private industry using Red-Teaming 3. Categorize according to vulnerability profiles 4. Assess likelihood of intentional tampering and relate causally to supply chain metrics 5. Determine synergies with reduction in theft and losses	1. Develop and validate models for assessing costs and benefits of security-related interventions 2. Value potential impacts from a security breach for each asset class • Direct/Indirect • Externalities • Monetary/non-monetary 3. Construct prioritization criteria such as Cost of security Breach to Likelihood ratio (CBL) 4. Prioritize efforts in various sectors and asset classes, e.g., according to CBL ratio	1. Analyze alternative strategies for DHS to reduce consequences of security breaches by direct action 2. Evaluate direct and indirect costs of best available private actions 3. Analyze alternatives to re-align public and private interests • Tax Incentives • Legal reform • Required Insurance 4. Evaluate costs and benefits of private-public partnership 5. Design audit system to monitor effectiveness and compliance

global supply chain that have the resources and the information to undertake necessary precautions locally, while assuring that larger problems or common problems and approaches are shared across the supply chain. An integrated approach such as that proposed in the present paper will be necessary in order to coordinate the very difficult process of risk assessment and risk management across such supply chains.

4. Strategic Dimensions, Actions and Conditions

Based on the analysis and empirical evidence presented above, two key dimensions emerge as fundamental in guiding management practice of disruption risk in supply chains. The first dimension consists of strategies and actions aiming at *reducing* the frequency and severity of risks faced, at both the firm level and across the supply chain. The second element focuses on *increasing* the capacity of supply chain participants (whether a separate firm or a subsidiary facility) to sustain/absorb more risk, without serious negative impacts, or major operational disruptions. Because disruption risks belong to the low-probability, high-consequence domain of outcomes, they cannot be managed in the traditional manner based on measuring outcomes and translating these into process improvements. Rather, the approach must be in the spirit of very high quality (six sigma) process management, in which the process itself is continually audited to assure a proper balance between risks and benefits of mitigation. In addition, we see in the chemical industry study that many disruptions risks involve a broader class of stakeholders than simply a company's owners/investors. They involve public sector regulators, employees and external stakeholders (e.g., in the arena of terrorism risks, regional, and national emergency response and law enforcement officials may also be involved). Because of this broader stakeholder involvement in many of the issues related to disruption risk management, special care must be exercised in the design of the management systems that have responsibility for assessment and mitigation of these risks. We have traced some elements of the emerging practice in this area in this paper.

What we see emerging is a two-fold approach, based on two levels of management systems. *First*, new systems are emerging for measuring and managing operational risks, and we have reviewed some of the progress being made in designing and implementing these systems. These systems, which generally go under the heading of "operational risk management," attend to the traditional tasks of identification, assessment, management and emergency response. *Second*, disruption risk management is now finding its way to the Board Room, especially in the aftermath of the terrorist attacks on the World Trade Center on 9/11/01. This is providing new visibility and coordination at the most senior levels of management on risks that may have significant consequences for the financial viability of the company. The systems and organizational procedures associated with this broader management activity go under the heading of integrated Enterprise Risk Management (ERM) systems. The challenges in managing disruption risks in supply chains encompass both levels of these management systems. Facilities and transportation links, as individual focal points for risk management, have been the first focus of supply chain disruption management systems, with implementation of vulnerability assessments, near-miss incident reporting systems, and emergency/crisis response procedures the initial focus of attention. Attention is now moving to supply chain wide systems, to promote visibility across the supply chain on major sources of disruption, and to promote the opportunity for joint problem solving across supply chain partners to implement best practices in the extended supply chain for identifying and managing disruption risks. Key challenges await both managers and researchers in this regard, as we attempt to discover cost-effective opportunities for risk mitigation while simultaneously providing the means to share the investment and insurance costs that must be in place to finance ex ante and ex post relief from the consequences of disruption. These are significant challenges because of the distributed ownership and globalization of many supply chains.

While the results and framework presented here provide a starting point for addressing these challenges, it is important to stress the importance of two final observations or "conditions" that are necessary for effective implementation:

Condition C1. The approaches used to mitigate disruption risks must "fit" the characteristics and needs of the underlying decision environment. Different supply chain environments will give rise to different approaches to assessment and mitigation. Even within a given sector such as mass retailers with global supply chains, the approaches taken by different companies will be different, given their differences in corporate culture and their methods of managing their supply chains. In the business of disruption risk management, one size will definitely not fit all.

Condition C2. Trust, information and continuing profitability are the basic glue that makes supply chain partnerships a reality. Continuous coordination, cooperation, and collaboration among supply chain partners are needed for risk avoidance, reduction, and mitigation such that the value and benefits generated are maximized and shared fairly. Different contractual and incentive schemes are now emerging as practical means toward this end. Linking risk assessment and risk management to identify vulnerabilities and opportunities for cost-effective mitigation is the first step in providing a rational basis for individual and group action among supply chain partners. Random investments or shots in the dark that do not properly account for the interdependencies across the supply chain will ultimately waste resources and destroy trust.

The principles articulated here, together with the established art and science of industrial risk management, provide a beginning point for the management of disruption risks in supply chains. On the conceptual side, our framework can be labeled as the "SAM-SAC" Framework, denoting the three main tasks of risk **S**pecification of sources and vulnerabilities, **A**ssessment, and **M**itigation, and the proposed **S**trategies with dual dimensions: **A**ctions and necessary **C**onditions for effective implementation. The refinement of the SAM-SAC approach, and the development of leading and lagging indicators of excellence in supply chain disruption management, for specific sectors and archetypes of supply chains present important challenges for research going forward.

Acknowledgments

The authors would like to thank the reviewers and the editor for their useful comments and suggestions that helped improve the content and readability of this paper. Helpful discussions with Caroline Beaird, Jack Harrald, Howard Kunreuther, Kalyan Singhal, Vinod Singhal, Jonathan Gold, and the participants of the Roundtable on Global Retail Chain Security on October 7, 2004 are also acknowledged. Remaining errors are the responsibility of the authors. Kleindorfer's research on this project was supported by a Cooperative Agreement with the U.S. Environmental Protection Agency and the Wharton-Columbia Radiant Trust Center of Excellence.

References

Agresti A. 2002. *Categorical Data Analysis*, 2nd ed. Wiley-Interscience, New York, New York.

Baiman, S., S. Netessine, H. Kunreuther. 2003. Procurement of quality in supply chains with a 'weakest link'. *Working Paper, Risk Management and Decision Processes Center,* The Wharton School, University of Pennsylvania.

Baird, I. S., H. Thomas. 1985. Toward a contingency model of strategic risk taking. *The Academy of Management Review* **10**(2) 230–243.

Balakrishnan, A., J. Geunes. 2004. Collaboration and coordination in supply chain management and e-commerce. *Production and Operations Management* **13**(1) 1–2.

Boyaci, T. G. Gallego. 2004. Supply chain coordination in a market with customer service competition. *Production and Operations Management* **13**(1) 3–22.

Buehler, K., G. Pritsch. 2003. Running with risk. *The McKinsey Quarterly*, No. 3.

Cachon, G. 2003. Supply chain coordination with contracts in *Handbooks in operations Research and Management Science: Supply Chain Management*, Chapter 11. S. Graves, deKok (eds.), North-Holland, Amsterdam.

Chase, R. B., N. J. Aquilano, F. R. Jacobs. 2004. *Operations Management for Competitive Advantage*, 10th ed. McGraw-Hill, Boston, Massachusetts.

Chopra, S., P. Meindl. 2003. *Supply Chain Management: Strategy, Planning and Operations*, 2nd ed. Prentice Hall, Upper Saddle River, New Jersey.

Corbett, C. J., M. J. Montes, D. A. Kirsch, M. J. Alvarez-Gil. 2002. Does ISO 9000 certification pay? *ISO Management Systems* July–August 31–40.

Elliot, M. R., P. R. Kleindorfer, R. A. Lowe. 2003. The role of hazardousness and regulatory practice in the accidental release of chemicals at US industrial facilities. *Risk Analysis* **23**(4) 865–881.

Elliot, M. R., Y. Wang, R. A. Lowe, P. R. Kleindorfer. 2004. Environmental justice: Frequency and severity of U.S. chemical industry accidents and the socioeconomic status of surrounding communities. *Journal Epidemiology and Community Health* **58**(1) 24–30.

Fine, C. H. 2000. Clockspeed-based strategies for supply chain design. *Production and Operations Management* **9**(3) 213–221.

Fisher, M., J. H. Hammond, W. Obermeyer, A. Raman. 1997. Configuring a supply chain to reduce the cost of demand uncertainty. *Production and Operations Management* **6**(3) 211–225.

Galbraith, J. R. 1973. *Designing Complex Organizations.* Addison-Wesley, Reading, Massachusetts.

Galbraith, J. R. 1977. *Organization Design*. Addison-Wesley, Reading, Massachusetts.

Gallagher, T. J., J. D. Andrew. 2000. *Financial Management: Principles and Practice*, 2nd ed. Prentice Hall, Upper Saddle River, New Jersey.

Gan, X., S. P. Sethi, H. Yan. 2004. Coordination of supply chains with risk-averse agents. *Production and Operations Management* **13**(2) 135–149.

Gan, X., S. P. Sethi, H. Yan. 2005. Channel coordination with a risk-neutral supplier and a downside risk-adverse retailer. *Production and Operations Management* **14**(1) 80–89.

Gerchak, Y. S. Wang. 2004. Revenue sharing versus wholesale price contracts in assembly systems with random demand. *Production and Operations Management* **13**(1) 23–33.

Grossi, P., H. Kunreuther (eds.). 2005. *Catastrophe Modeling: A New Approach to Managing Risk.* Springer-Verlag, Heidelberg, Germany.

Haimes, Y. Y. 1998. *Risk Modeling, Assessment, and Management.* Wiley and Interscience, New York, New York.

Handfield, R. B., E. L. Nichols. 2002. *Supply Chain Redesign: Transforming Supply Chains into Integrated Value System*, 1st ed. Prentice Hall, Upper Saddle River, New Jersey.

Harrald, J. R. 2002. Corporate Business Continuity and Crisis Management as a Strategic Function, Working Paper. The George Washington University, December.

Hendricks, K. B., Singhal, V. R. 2005. The effect of supply chain glitches on shareholder wealth. *Journal of Operation Management* **21**(5) 501–523.

Hendricks, K. B., Singhal, V. R. 2005. An empirical analysis of the effect of supply chain disruptions on long-run stock price and equity risk of the firm. *Production and Operations Management* **14**(1) 35–52.

Hertz, D., H. Thomas. 1984. *Practical Risk Analysis: An Approach Through Case Histories.* Wiley, Chichester, New York.

Holmstrom, B. 1982. Moral hazard in teams. *Bell Journal of Economics* **13**(2) 324–340.

Huchzermeier, A., M. A. Cohen. 1996. Valuing operational flexibility under exchange rate uncertainty. *Operations Research* **44**(1) 100–113.

Kleindorfer, P. R. 1997. Market-based environmental audits and environmental risks: Implementing ISO 14000. *The Geneva Papers on Risk and Insurance* **22**(83) 194–210.

Kleindorfer, P. R. 2001. Industrial Ecology and Risk Analysis in *Handbook of Industrial Ecology*, L. Ayres, R. Ayres (eds.), Elsevier.

Kleindorfer, P. R., J. C. Belke, M. R. Elliot, K. Lee, R. A. Lowe, H. Feldman. 2003. Accident epidemiology and the U.S. chemical industry: Accident history and worst-case data from RMP*Info. *Risk Analysis* **23**(5) 865–881.

Kleindorfer, P. R., M. R. Elliot, Y. Wang, R. A. Lowe. 2004. Drivers of accident preparedness and safety: Evidence from the RMP Rule. *Journal of Hazardous Materials* **115** (August) 9–16.

Kleindorfer, P. R., H. C. Kunreuther, P. J. Shoemaker. 1993. *Decision Sciences: An Integrative Perspective.* Cambridge University Press, Cambridge, Massachusetts.

Kleindorfer, P. R., E. W. Orts. 1998. Informational regulation of environmental risks. *Risk Analysis* **18**(2) 155–170.

Kleindorfer, P. R., Van Wassenhove, L. 2004. Risk management for global supply chains: An overview in *The Alliance on Globalizing*, Chapter 12. H. Gatignon, J. Kimberly (eds.). Cambridge University Press, Cambridge, Massachusetts.

Kleindorfer, P. R., D. J. Wu. 2003. Integrating long-term and short-term contracting via business-to-business exchanges for capital-intensive industries. *Management Science* **49**(11) 1597–1615.

Kraiselburd, S., V. G. Narayanan, A. Raman. 2004. Contracting in a supply chain with stochastic demand and substitute products. *Production and Operations Management* **13**(1) 46–62.

Kunreuther, H. G. Heal. 2004. Interdependent security: The case of identical agents. *Journal of Risk and Uncertainty* **23**(2) 103–120.

Lasher, W. R. 2003. *Practical Financial Management*, 3rd ed. Thomson/South-Western, Mason, Ohio.

Lee, H. L., S. Whang. 2003. Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management. Research Paper No. 1824, Stanford University, Stanford, Connecticut, October.

Lee, H. L., M. Wolf. 2003. Supply chain security without tears. *Supply Chain Management Review* **7**(1) 12–20.

Lee, H. L. 2002. Aligning supply chain strategies with products uncertainties. *California Management Review* **44**(3) 105–119.

Levi, M., P. R. Kleindorfer, D. J. Wu. 2003. Codifiability, relationship-specific information technology investment, and optimal contracting. *Journal of Management Information Systems* **20**(2) 77–100.

Martinez-de-Albeniz, V., D. Simchi-Levi. 2005. A portfolio approach to procurement contracts. *Production and Operations Management* **14**(1) 90–114.

Michaels, J. V. 1996. *Technical Risk Management.* Prentice Hall, Upper Saddle River, New Jersey.

Monczka, R., R. Tent, R. Handfield. 2002. *Purchasing and Supply Chain Management* 2nd ed. South-Western, Cincinnati, Ohio.

Papadakis, I. S., W. T. Ziemba. 2001. Derivative effects of the 1999 earthquake in Taiwan to U.S. personal computer manufacturers in *Mitigation and Financing of Seismic Risks.* P. R. Kleindorfer, M. R. Sertel (eds.), Kluwer Academic Publishers, Boston, Massachusetts.

Pauchant, T. C., I. I. Mitroff. 1992. *Transforming the Crisis-Prone Organization: Preventing Individual, Organizational, and Environmental Tragedies.* Jossey-Bass, San Francisco, California.

Perrow, C. 1999. *Normal Accidents: Living with High Risk Technologies.* Princeton University Press, Princeton, New Jersey.

Phimister, J. R., U. Oktem, P. R. Kleindorfer, H. Kunreuther. 2003. Near-miss incident management in the chemical process industry. *Risk Analysis* **23**(3) 445–459.

Rice, J. B., Caniato, J. Fleck, D. Disraelly, D. Lowtan, R. Lensing, C. Pickett. 2003. Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains. MIT Center for Transportation and Logistics Report, August.

Robb, S. P., A. Bailey. 2003. *Risky Business: Corruption, Fraud, Terrorism & Other Threats to Global Business*, Revised edition. Kogan Page Ltd., London, United Kingdom.

Saad, G. H. 2003. Transformation of Supply Chain Management Challenges into Business Opportunities, Association of Pennsylvania Universities Business and Economics Faculty (*APUBEF*) Proceedings. forthcoming.

Saad, G. H. 2001. Strategic performance evaluation: A descriptive and prescriptive analysis. *Journal of Industrial Management* **101**(8/9), 390–399.

Saad, G. H., S. Siha. 2000. Managing quality: Critical links and a contingency model. *International Journal of Operations and Production Management* **20**(10) 1146–1163.

Souza, G. C., Z. Zhao, M. Chen, M. O. Ball. 2004. Coordinating sales and raw material discounts in a global supply chain. *Production and Operations Management* **13**(1) 4–45.

Sodhi, M. S. 2005. Managing demand risk in tactical supply chain planning for a global consumer electronic company. *Production and Operations Management* **14**(1) 69–79.

Shavell, S. 1984. A model of the optimal use of liability and safety regulation. *Rand Journal of Economics* **15**(2) 271–280.

Stevenson, W. J. 2004. *Operations Management,* 8th ed. McGraw-Hill/Irwin, New York, New York.

Upton, D. M. 1998. *Designing, Managing, and Improving Operations.* Prentice Hall, Upper Saddle River, New Jersey.