The Weakest Link: Managing Risk Through Interdependent Strategies

Howard Kunreuther
The Wharton School
University of Pennsylvania

in
The Network Challenge: Strategy, Profit and Risk in an Interlinked World
Paul R. Kleindorfer and Yoram Wind (eds.)
Wharton School Publishing, Upper Saddle River, NJ: 2009.

THE WHARTON RISK MANAGEMENT AND DECISION PROCESSES CENTER

Established in 1984, the Wharton Risk Management and Decision Processes Center develops and promotes effective corporate and public policies for low-probability events with potentially catastrophic consequences through the integration of risk assessment, and risk perception with risk management strategies. Natural disasters, technological hazards, and national and international security issues (e.g., terrorism risk insurance markets, protection of critical infrastructure, global security) are among the extreme events that are the focus of the Center's research.

The Risk Center's neutrality allows it to undertake large-scale projects in conjunction with other researchers and organizations in the public and private sectors. Building on the disciplines of economics, decision sciences, finance, insurance, marketing and psychology, the Center supports and undertakes field and experimental studies of risk and uncertainty to better understand how individuals and organizations make choices under conditions of risk and uncertainty. Risk Center research also investigates the effectiveness of strategies such as risk communication, information sharing, incentive systems, insurance, regulation and public-private collaborations at a national and international scale. From these findings, the Wharton Risk Center's research team – over 50 faculty, fellows and doctoral students – is able to design new approaches to enable individuals and organizations to make better decisions regarding risk under various regulatory and market conditions.

The Center is also concerned with training leading decision makers. It actively engages multiple viewpoints, including top-level representatives from industry, government, international organizations, interest groups and academics through its research and policy publications, and through sponsored seminars, roundtables and forums.

More information is available at http://opim.wharton.upenn.edu/risk.

Chapter 22
The Weakest Link: Risk Management Strategies for Dealing with Interdependencies

Howard Kunreuther[1]

Abstract

Networks increase interdependencies and this creates challenges for managing risks. This is especially apparent in areas such as security and enterprise risk management, where the actions of a single player in an interconnected network can wreak havoc on everyone in the network. The network, in this case, is only as strong as its weakest link. There are related problems in encouraging investments for prevention and protection, since the expected payoffs from such measures by one player are affected by the actions of other players in the network. In this chapter, Howard Kunreuther examines the challenges of interdependent security (IDS) and strategies for addressing these, including coordination with broader networks such as industry organizations and government.

On December 21, 1988, Pan Am flight 103 exploded near Lockerbie, Scotland. Terrorists had checked a bag containing a bomb in Malta on Malta Airlines, which had minimal security procedures. The bag was transferred in Frankfurt to a Pan Am feeder line, and then loaded onto Pan Am 103 in London's Heathrow Airport. The bomb was designed to explode above 28,000 feet, a height normally first attained on this route over the Atlantic Ocean. Given such interdependencies among different players in a network, the above example illustrates that security for the entire network may only be as strong as its weakest link. In this case, the terrorists deliberately exploited the widely varying security procedures across the airlines. This problem is common to other transportation modes, where there are interconnections between nodes in the network.[2]

Interdependencies create a challenge for airlines in making decisions about investing in security. An airline knows that if it invests in baggage security it may face a security risk from a dangerous bag loaded onto its plane by another airline. It faces this risk unless it inspects all transferred bags, a policy until recently only followed by El Al airlines.

In a networked world, the risks faced by any one agent depend not only on that agent’s own choices but also on those of others. More specifically, the economic incentive of any agent to invest in protection depends on how she expects others to behave. The strategies can be risk-reducing measures as well as information-gathering and preparedness activities. The fact that such events are typically probabilistic, and that the risk that one agent faces is often determined in part by the behavior of others, gives a unique and complex structure to the incentives that agents face to reduce their exposures to these risks that come under the heading of interdependent security (IDS).

For many IDS problems, if an agent thinks that others will *not* invest in protection, then this reduces the incentive for her to do so. On the other hand, should she believe that others will invest in security, it may be best for her to do so also. So, it is often the case that there are two equilibria: (1) no one invests in protection, even though all would be better off if they had incurred this cost or (2) everyone invests in protection. In some cases, there may be incentives that can push the system past a tipping point where it shifts from the first equilibrium to the second.

This chapter characterizes the nature of the interdependency problem and suggests risk management strategies for improving both individual and social outcomes. The first section outlines a series of IDS scenarios to illustrate the range of problems that fall under this rubric. The second section focuses on the problem of a firm with more than one decentralized division, using a simple game theoretic model to illustrate how the expected profits of each division would be improved had all of them invested in risk-reducing measures. The third section introduces risk management strategies to improve individual and social welfare. We examine how one might induce tipping or cascading by either subsidizing or fining one of the divisions so that it has an economic incentive to invest in protection, leading the others to follow suit. In particular, I focus on coordination measures within a decentralized firm (e.g., creating a corporate culture focused on managing low-probability, high-consequence events) as well as within an industry (e.g., private trade associations) to induce cooperative behavior. The public sector can also play an important role through interventions such as taxes, subsidies, insurance and regulations to deal with the negative externalities caused by interdependent security. The paper concludes with suggestions for future field and experimental research in this area and final comments.

IDS SCENARIOS

In addition to the airline security case discussed above, the challenge of interdependent risks can be seen in many areas. In the following scenarios, weak links in the system may lead to suboptimal behavior by everyone. These cases also illustrate possible solutions to address these interdependent risks.

Example 1: Protection of Shared Network Resources[3]

Many workplaces have a complex network of shared resources (such as files, disks, peripheral devices, and bandwidth) along with individual resources (such as desktop machines). The vulnerability of the shared resources to various security risks often depends strongly on the collective actions used to protect individual resources. For example, a shared disk may be erased by a virus entering the local network through the desktop machine of a user who failed to update his or her anti-virus software signatures. Individual actions also affect shared resources such as bandwidth. For example, users whose machines are infected with a variety of “malware” can surreptitiously consume huge amounts of bandwidth, at the expense of all other users of the system. Such problems are common among residential commercial cable subscribers to Internet access**.**

Example 2: Global Supply-Chain Management[4]

Global supply chains face risks from terrorists and other disruptions. One weak link is enough to allow a purposeful agent to penetrate the supply chain and to undermine the risk mitigation actions of all others in the supply chain (Heal et al. 2006). Making these global supply chains less vulnerable depends upon the actions of many players. Spurred by the concerns of the new U.S. Department of Homeland Security's (DHS's) for protecting critical infrastructure, major retailers, and transportation and logistic specialists came together in 2002 to discuss the responsibilities of the private and public sectors in meeting the new challenges of interdependent security in global supply chains. These early discussions were eventually synthesized in the United States into a voluntary public--private partnership approach to cargo security called the Customs--Trade Partnership Against Terrorism (C-TPAT). The idea of C-TPAT was to develop basic principles, and associated best practices, for all participants in a global supply chain in four areas: site security, personnel (including background checks), material movements, and process control (Kleindorfer and Saad 2005). C-TPAT is designed to integrate the activities of three types of actors: private companies who manufacture and move cargo; port authorities and de-consolidators; and local, regional and national agencies responsible for homeland security.

Example 3: Meltdown of a Nuclear Reactor[5]

Assume that each country has one nuclear reactor, and that if it invests in a set of safeguards, the chances of an accident from the power plant are reduced to zero. We imagine a group of small adjacent countries (e.g., Belgium, Holland, and Luxembourg, or Latvia, Lithuania, and Estonia), where a meltdown in any one will lead to radioactive contamination in all of them. What role could international compacts or trade associations play to ensure that all countries invest in safeguards? A related issue is the ripple effects from an accident that does not result in contamination. For example, in the U.S., an accident at any one plant is likely to lead to costly regulatory interventions at all plants. That is why the Institute of Nuclear Power Operations was founded after the incident at Three Mile Island—to serve as a self-policing arm for the industry, so that well-performing plants would not be held hostage to the safety problems of plants with poorer safety records.

Example 4: Environmental Treaties[6]

Suppose that countries are asked to sign a treaty to reduce some environmental risk, such as global warming or atmospheric pollution. There is a net cost to any one country for adopting the treaty, but potential benefits to the entire planet if enough countries take this action. What incentive is there for any one country to adopt the treaty if it knows that a number of other countries will not join? How can one convince countries with leverage to sign the treaty to induce others to follow suit? There are equity-efficiency tradeoffs.

For example, it might be economically more efficient for only a subset of countries to take preventive actions by being part of a treaty, but more equitable and politically saleable for all countries to sign the treaty.

Example 5: Interdependent Critical Infrastructures[7]

As shown by disasters such as 9/11 and Hurricane Katrina, the failure of infrastructure in one sector can lead to disruptions in other sectors. For example, financial systems and emergency services are highly dependent on telecommunication operations, which are highly dependent on electricity. In a system such as a power grid, there is a systematic tendency to under-invest in reliability, individual capacity or security measures such as trimming vegetation near distribution lines to reduce the chance of a power failure. The costs of failure are passed on to competitors and customers in other parts of the network. When the interdependencies cut across sectors, the nature of the risks are often not well understood so that they pose special policy challenges. The private and public sector share an interest in making social and economic systems less vulnerable to disasters. There is growing interest in protecting critical infrastructure to assure the social and economic continuity of the nation (transportation, water distribution, telecommunication, electricity, emergency services, financial services, etc.) in the event of terrorist attacks or severe natural hazard events.

Example 6: Protecting a Firm against Catastrophic Losses[8]

For large corporations, a failure in one part of the world or one division can lead to disruption or bankruptcy of the entire firm nationwide or even worldwide. For example, a Bhopal-like accident at a chemical plant can lead to losses that are so large that they cause bankruptcy of the entire operation. An ownership group such as Lloyd's, which controls a number of semi-autonomous syndicates, can fail if one of the syndicates experiences a severe enough loss. In February 1995 Barings Bank was destroyed by the actions of a single trader in its Singapore unit and in 2002 Arthur Andersen was sent into bankruptcy by the actions of its Houston branch working with Enron.Similar events have happened to other financial services units in recent years and months notably the potential collapse of the American International Group (A.I.G.), the world's largest insurer, as a result of a 377-person London Unit known as A.I.G. Financial Products that was run with almost complete autonomy from the parent company (Morgenson 2008). Given such an institutional structure, what economic incentive does any division have to incur the costs of protective measures that adversely affect its balance sheet, if other divisions in the organization are not taking similar actions? A culture of risk-taking can spread through the firm, because knowledge that a few groups are taking large risks reduces the incentives that others have to manage their operations carefully.

CHARACTERIZING THE PROBLEM—INVESTING IN A CHEMICAL PLANT

How can these interdependent risks be addressed? As illustrated by some of the examples above, in many cases this is done by looking to the network itself. There may be ways of inducing tipping and cascading so that everyone's welfare is improved. One may then want to determine the nature of critical coalitions that can tip the entire system. Is there any agent (e.g., firm, individual) or group of agents one should focus attention on? More generally, what types of private sector coordination measures (e.g., private trade associations) and public sector interventions such as taxes, subsidies, fines, regulations and well-enforced standards are appropriate for dealing with the negative externalities caused by interdependent security?

To illustrate an approach to addressing interdependent risks, consider a simplified case of a single firm with several divisions (as discussed in Example 6). The BeSafe chemical firm has two identical independently operating divisions, each maximizing its own expected returns and having to choose whether to invest in a protective measure. Such an investment would reduce the probability of a catastrophic chemical accident to one of its plants. Suppose Division 1 has invested in protection. There is still an additional risk that BeSafe will go bankrupt if Division 2 has not taken this precautionary measure. In other words, the employees in Division 1 may lose their jobs because of the carelessness of Division 2. In this sense, Division 2 can contaminate other parts of the organization by *not* protecting its plants against a catastrophic accident. Similarly, Division 1 can contaminate Division 2 if it fails to adopt adequate protection.

From Division 1's perspective, adding a second division creates the possibility of contamination and reduces its incentive to invest in protection. Why? Because in isolation, investment in protection buys the employees in Division 1 freedom from bankruptcy. With the possibility of contamination from others, it does not. Even after investment there remains a risk of bankruptcy from the other division. Investing in protection buys you less when there is the possibility of contamination from others.

The results for the two-division case carry over to more general settings with some increase in complexity. The incentive for any agent to invest in protection depends on how many other agents there are and on whether or not they are investing. Other agents who do not invest reduce the expected benefits from each division's own protective actions and hence reduce any single division's incentive to invest.

Suppose there are *n* divisions in the firm. If *n* is large and none of the other *n-1* divisions have invested in protection, it is highly unlikely that your division will want to invest in protecting itself against a catastrophic accident. Here is the intuition for this somewhat surprising result. One weak link in the organization compromises all the other divisions. In other words, one unprotected division endangers all of the other divisions in the firm even if they have all invested in security. The more divisions that have not invested in protection, the greater the chances that the employees of any division will be looking for another job even if its own plants are secure from a catastrophic accident. As more divisions decide *not* to invest in security, the probability of a catastrophic accident becomes greater and there is even less economic incentive for your division to undertake protection. This sets up a negative cycle that leads to declining investments in protection. But the reverse can also be true. If more players invest in protection, there is a greater incentive for others to do so, and, above a certain threshold, this can lead to a positive and reinforcing cycle of investment incentives, as discussed below.

Understanding the risks facing individual nodes and the entire network demands rigorous risk assessment and knowledge of varying risk perceptions. As BeSafe collects more accurate information on the risks of chemical accidents at each of its chemical plants, it can develop more effective strategies for planning at its different divisions. Risk perceptions may also vary across the network, and will affect investments in prevention. For example, some managers at BeSafe might only invest in preventive actions if they perceive that the chance of some event rises above some probability level.

DEVELOPING RISK MANAGEMENT STRATEGIES: TIPPING AND CASCADING[9]

With the right incentives, the network itself can encourage actions by individuals that reduce collective risks. Tipping refers to a situation where a switch of strategy by a small group of agents will lead all (or most of) the others to follow suit. In the context of the BeSafe chemical plant example, cascading implies that if one division invests in protection, one or more (but not all) other divisions will do the same, inducing others to invest in protection (Dixit 2002). There will be some divisions in an organization that may produce much greater negative externalities by their actions than others. For example, a large division that went bankrupt would be much more likely to cause other divisions to follow suit than a smaller unit in the organization. The large division could suffer a catastrophic loss from an accident that would have much more serious repercussions than if the accident occurred at a smaller plant. By providing incentives for the large division to invest in protection one may convince others in the organization to do the same.

If there is a weak link in the network that can cause severe disruptions to others, it may only be necessary to provide economic incentives to this unit to improve its profitability as well as all of the others in the system through a tipping or cascading process. It is this weak link property that characterizes many practical problems in interdependency and can have major impacts on others members of the network.

Tipping has been documented in many contexts. Thomas Schelling’s work highlights this point (Schelling 1978). He provides an example of a sudden change in the racial composition of a neighborhood. Non-whites gradually move into an originally white neighborhood: when the proportion reaches a critical level, the neighborhood tips and the remaining whites all move out together (Schelling 1971).

Creating Incentives for Tipping

Once a point of tipping or cascading is reached, individuals in the network will often begin making their own investments in protection. How can this tipping point be encouraged? Coordinating mechanism and incentives – often through private-public partnerships – can create an environment in which individuals have more incentive to invest in protection.

Internal Organizational Rules and Other Coordinating Mechanisms

A large decentralized firm with many divisions will likely need some type of coordinating mechanism from top management to encourage investments if each division's objective is to maximize the expected returns of its own employees. A key question in this regard is how companies who advertise, "Safety is our most important product" actually operationalize this slogan. Larger firms in the chemical industry have formed functional units that play this role across the organization. For example, DuPont has a process safety management group that is responsible for making sure that all the different divisions in the firm follow appropriate procedures.

In the context of the BeSafe example, the company could set up such a cross-cutting unit and institute a specific rule that would require divisions to invest in protective measures when the expected benefits to the firm exceeded the costs of the measure. One way to determine what type of rule to enforce is to consider catastrophic accidents that caused losses so large that it would threaten the solvency of the firm but where the division itself would not want to incur the costs of investing in protective measures.

Role of the Public Sector

The public sector can play an important role in protection, and has an interest in doing so in areas such as chemical safety where a company's actions can affect people off-site. A company such as BeSafe may not be held fully liable for the consequences of a chemical accident. For example, the firm causing an accident may not be legally responsible for losses from related decreases in property values of surrounding homes or disruptions in community life.

One way for the government to enforce its regulations is to turn to the private sector for assistance. More specifically, third party inspections coupled with insurance protection can encourage divisions in firms to reduce their risks from accidents and disasters. Such a management-based regulatory strategy shifts the locus of decision-making from the regulator to firms, which are now required to do their own planning to meet a set of standards or regulations. (Coglianese and Lazer, 2003)

The passage of Section 112(r) of the Clean Air Act Amendments (CAAA) of 1990 offers an opportunity to implement such a program. This legislation required facilities to perform a hazard assessment, estimate consequences from accidents and submit a summary report to the U.S. Environmental Protection Agency (EPA) called the Risk Management Plan (RMP) (Belke, 2001). The challenge currently facing the EPA is how to encourage compliance with these regulations so that firms will improve safety.

There is some urgency for a type of decentralized procedure with appropriate incentives due to the EPA's limited personnel and funds for providing technical guidance and auditing regulated facilities. Chemical firms, particularly smaller ones, have little financial incentive to follow centralized regulatory procedures if they estimate that the likelihood they will be inspected by a regulatory agency is very small and/or they face a low fine if caught. In such cases, they may be willing to take their chances and incur the fine should they be caught violating the rule or regulation. This is like putting money into a parking meter. If you know that the chances of a meter being checked are very low and the fine is relatively small, then you might think twice before parting with your quarters.

The combination of these two market mechanisms – third-party inspections and private insurance – creates a powerful incentive for firms to implement RMPs to make their plants safer. It also encourages the remaining firms to comply with the regulation to avoid being caught and fined. The intuition behind using third parties and insurance to support regulations can be stated rather simply when the regulatory agency has limited personnel to enforce its own rules: low-risk divisions, which the EPA has no need to audit, cannot credibly distinguish themselves from the high-risk ones without some type of inspection.[10]

By delegating part of the inspection process to the private sector through insurance companies and third parties, the EPA provides a channel though which the low-risk divisions in firms can speak for themselves. If a division chooses not to be inspected by third parties, it is more likely to be a high-risk rather than a low-risk one. If it does get inspected and shows that it is protecting itself and the rest of the organization against catastrophic accidents, it will pay a lower premium than a high-risk division which is not undertaking these actions. In this way, the proposed mechanism not only substantially reduces the number of inspections the EPA has to undertake, but it also makes their audits more efficient.

Kunreuther, McNulty and Kang (2002) show more formally how such a program could be implemented in practice. They provide supporting evidence from pilot studies by the Department of Environmental Protection in Delaware and Pennsylvania, which worked closely with the insurance industry and chemical plants in testing the proposed program. Similar studies for small firms were undertaken by McNulty et al. (1999).

The process safety management unit of a firm should support this program for two reasons. It provides a rationale for the firm to hire third-party inspectors to make sure their divisions are operating safely. The program also increases the firm's expected profits by reducing the negative externalities that divisions create due to their fear of being contaminated by others.

FUTURE RESEARCH [11]

The problem of assessing and managing risks when interdependencies and network effects are present highlights the importance of undertaking research on both the descriptive and prescriptive aspects of decision making for low-probability, high-consequence events. It also presents new challenges for the foundations of risk and security management in the presence of network interdependencies. Using the BeSafe chemical company example as background, we consider these challenges under the headings of risk assessment, risk perception, and risk management.

Risk Assessment

First, we need to collect better data to estimate the risks and consequences of a catastrophic accident. The Wharton Risk Management and Decision Processes Center has analyzed accident history data from the U.S. chemical industry (Kleindorfer et al. 2007). These accident history data can be linked to financial information so one can analyze the association, if any, between the financial characteristics of the parent company of a facility and the frequency or severity of accidents. Similarly, the property damage estimates, and associated indirect costs from these, can be used to assess the consequences of environmental health and safety incidents on overall company performance and provide valuable insights for insurance underwriting for such accidents. Finally, the same data can be used to assess worst-case consequences from such incidents, including those that might arise from site security risks associated with terrorism.

The second data collection project is a study of “near misses” in organizations and the systems that have been put into place to report and analyze these data (Phimister et al., 2003). Near misses are defined as incidents that, under different circumstances, could have resulted in major accidents. Linking these data on accident precursors to the Accident History database may enable one to identify categories of precursors that give early warnings of the potential for major accidents. Audit tools and other aspects of near-miss management can then focus not just on emergency response but on the range of prevention and mitigation activities before the fact that can help avert major disasters. Even with these data, there will still be considerable uncertainty regarding the estimates of risks associated with these low-probability events (National Academy of Engineering 2004).

Risk Perception

Second, we need more research on how risk interdependencies affect firms’ decision processes. The IDS models developed to date assume that individuals or firms make their decisions by comparing expected benefits with and without protection to the costs of investing in security. There is a growing literature in behavioral economics that suggests that individuals and firms make choices in ways that differ from such a rational model of choice (Kahneman and Tversky, 2000). For example, there is evidence that people are myopic and do not appropriately take into account the long-term benefits of investing in protective measures, preferring instead to have a return on their investments over a relatively short time period. Such short-term horizons may work against protection and prevention measures for low-probability, high-consequence events by the very nature of these events. It would be useful to understand what factors motivate managers’ behavior and to consider strategies for making the investment more worthwhile. Some type of accounting arrangement by the firm to convert the upfront payment into a loan arrangement, for example, may enable managers to justify the upfront costs while relieving the division of budget constraints that may deter them from making the investment.

We also need to better understand how managers process information on risk when there is considerable uncertainty on the likelihood or consequences of an accident. We know that individuals have a difficult time dealing with ambiguous risks, particularly those of the low-probability variety (Slovic, 2000). One telling example is the way the chemical industry behaved prior to and after the Bhopal disaster. Prior to the accident, there was a tendency to treat an accident such as the one that occurred in the Union Carbide plant in India as one that will not happen to “our firm.” Following the disaster, all chemical companies undertook a detailed study of chemicals with catastrophic risk potential and took special measures to deal with them (Bowman and Kunreuther, 1988).

Risk Management

Third, with respect to managing risks, we need to understand the impact of certified information, including audits, on behavior and outcomes in risky environments. For the chemical industry, for example, third-party inspection may serve the double purpose of providing information on the level of risk of particular installations as well as providing a signal to insurers and regulators on premiums and inspection levels for firms that invest in protective measures. Incentives implied by improved alignment of insurance premiums with the level of risk of a company can play an important role in inducing investments in risk reduction. Reliable third-party inspections can provide the necessary certification that the chemical firm has an appropriate risk management plan and is operating in a safe manner. Regulatory agencies and public interest groups may also find the audits/inspections to be of value, knowing that insurers and auditors are concerned with their own bottom line and would have no incentive to classify a firm as *not risky*, if in fact it posed a high risk.

Another area that needs to be examined more carefully is the role that certifications, such as ISO14000, can play in encouraging firms and divisions to operate more safely. In a recent analysis of ISO data and firm performance, Kang (2005) has shown that facilities that have had serious environmental problems were more likely to arrange to be ISO14000 certified than lower-risk facilities and that their performance improved over the other facilities in the industry after they were certified. There is a tendency for many facilities in a firm to undertake ISO14000 certification procedures at approximately the same time, suggesting that organizations are using this standard as a way of forcing many of their facilities to undergo an inspection that they might otherwise not consider.

Finally, there may be an important role that trade associations can play in providing guidelines for firms to follow with respect to their operations. The American Chemistry Council (ACC), an association of chemical manufacturers, has undertaken this role through its Responsible Care initiative. Since 1988, members of the ACC have significantly improved their environmental, health, safety and, in recent years, security performance through the Responsible Care initiative. Participation in Responsible Care is mandatory for ACC member companies, all of which have made CEO-level commitments to uphold requirements that include a management system to drive environmental, health, safety and security performance, sharing progress and activities with the public and having mandatory certification by independent, accredited auditing firms.[12]

CONCLUSION: USING NETWORKS TO ADDRESS RISKS

Research in these areas can improve our understanding of the nature of interdependent risks and the effectiveness of strategies to address them. These risks arise in the context of networks, so we need to understand network relationships and interactions to understand the true nature of the risks. This requires assessing the risks of individual players and how their actions affect one another. As with the case of airline security discussed in the opening of this chapter, one weak link can erode the security of the entire network and create disincentives for individual investments in protective measures.

Since these risks arise within interdependent networks, effective solutions usually demand looking beyond an individual firm or division. These solutions may involve coordinating efforts across divisions in a firm, across a supply chain, or across the public and private sectors to create a context and supporting information for individual actions that decrease collective risk. These incentives can push the network to a tipping point or cascade that then reinforces behavior that benefits the entire network. The challenge of interdependent risks derives from network interactions. It is therefore not surprising that efficient solutions to these problems of interdependency require understanding and harnessing the power of the network itself.

REFERENCES

Auerswald, P., L. Branscomb, T. LaPorte, and E. Michel-Kerjan, (2006) *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. New York: Cambridge University Press.

Barrett, S. *Environment and Statecraft: the Strategy of Environmental Treaty-Making* Oxford University Press, (2003)

Belke, J. (2001), "The Case for Voluntary Third Party Risk Management Program Audits." Paper presented at the 2001 Process Plant Safety Symposium of the American Institute of Chemical Engineers, April 23.

Bowman, E.H. and H. Kunreuther, (1988), "Post Bhopal Behavior of a Chemical Company," *Journal of Management Studies*, 25, 387-402.

Coglianese, C. and D. Lazer, (2003), "Management-Based Regulation: Prescribing Private Management to Achieve Public Goals" *Law and Society Review* 37: 691-730

Cohen, M. and H. Kunreuther (2007) "Operations Risk Management: Overview of Paul Kleindorfer's Contributions," *Production and Operations Management*, 18(5), 525-541.

Dixit A. K. (2002). "Clubs with Entrapment," *American Economic Review* 93: 1824-1829.

Greenwald, B. and J. Stiglitz, (1990), "Asymmetric Information and the New Theory of the Firm: Financial Constraints and Risk Behavior," *American Economic Review: Papers and Proceedings* 80:160-165.

Heal, G. and H. Kunreuther, (2005a), "IDS Models of Airline Security" *Journal of Conflict Resolution* 41:201-17.

Heal, G. and H. Kunreuther, (2005b) "You Can Only Die Once" in H.W. Richardson, P. Gordon and J.E. Moore II, (eds.), *The Economic Impacts of Terrorist Attacks.* Cheltenham, UK: Edward Elgar.

Heal, G., M. Kearns, P. Kleindorfer and H. Kunreuther (2006), "Interdependent Security in Interconnected Networks," in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, P. Auerswald, L. Branscomb, T. LaPorte, and E. Michel-Kerjan, (eds.) New York: Cambridge University Press.

Kahneman, D. and A. Tversky, (2000) *Choices, Values and Frames* New York: Cambridge University Press.

Kang, Y. (2005) “The Impacts of Third Party Inspections on Industrial Safety and Environmental Performance” Philadelphia: Wharton School, University of Pennsylvania (mimeo)

Kearns, M (2005). "Economics, Computer Science, and Policy.” *Issues in Science and Technology*, Winter 37-47.

Kleindorfer, P.R., Rosenthal, R. Lowe, R.A., Fu, R and Belke, J. (2007) *Accident epidemiology and the RMP Rule: Learning from a decade of accident history from the U.S. Chemical Industry* Philadelphia: Wharton Risk Management and Decision Processes Center Report December 20.

Kleindorfer, P. R. and G. H. Saad, (2005) “Managing Disruption Risks in Supply Chains,” *Production and Operations Management*, 14(1): 53-68.

Kunreuther, H and G. Heal (2003),”Interdependent Security,” *Journal of Risk and Uncertainty,* (2003) Springer vol. 26(2-3) pp. 231-49.

Kunreuther, H, and G. Heal, (2005). “Interdependencies in Organizations,” in B. Hutter and M. Powers (eds.) *Organizational Encounters with Risk*, Cambridge: Cambridge University Press.

Kunreuther, H., P. McNulty, and Y. Kang, (2002), “Improving Environmental Safety through Third Party Inspection,” *Risk Analysis* 22:309-18

McNulty, P., R.A. Barrish, R.C. Antoff, and L.C. Schaller, (1999), “Evaluating the use of third parties to measure process safety management in small firms.” 1999 Annual Symposium, Mary Kay O’Connor Process Safety Center, Texas A&M University, October 26.

Morgenson, G. “Behind Insurer’s Crisis, Blind Eye to a Web of Risk” *New York Times* (September 28 2008) p. 1.

National Academy of Engineering (2004) *Accident Precursor Analysis and Management*, Washington DC, The National Academies Press.

Phimister, J., Oktem, U., Kleindorfer, P. and Kunreuther, H. (2003) “Near-Miss Incident Management in the Chemical Process Industry,” *Risk Analysis*, 23: 445-459.

Schelling, T. (1971). "Dynamic Models of Segregation" *Journal of Mathematical Sociology* 1:143-86.

Schelling, T. (1978). *Micromotives and Macrobehavior*. New York: Norton

Slovic, P. (2000). The *Perception of Risk.* London, UK: Earthscan.

NOTES

[1] Cecilia Yen Koo Professor of Decisions Sciences and Public Policy at the Wharton School, University of Pennsylvania and co-director of the Wharton Risk Management and Decision Processes Center.
E-mail address: Kunreuther@wharton.upenn.edu

[2] See Heal and Kunreuther (2005a) for more details on this scenario and a formal game theoretic model of the problem.

[3] See Heal et al. (2006) and Kearns (2005) for more details on this scenario

[4] See Heal et al. (2006) for more details on this scenario

[5] See Heal and Kunreuther (2005b) for more details on this scenario

[6] See Barrett (2003) for more details on this scenario

[7] See Auserwald et al. (2006) for more details on this scenario

[8] See Kunreuther and Heal (2005b) for more details on this scenario

[9] This section is based on material in Kunreuther and Heal (2005b).

[10] The same logic of third-party inspections has been implemented in many domains. Perhaps the best known of these is the ISO 9000 quality standard. Such international standards are intended to reinforce best practices across organizations. These standards are almost always backed by audits as a means of assuring compliance with the standard. Research on ISO 14000 is discussed further below. For information on the standards development process at the International Standards Organization (ISO), see http://www.iso.org/iso/home.htm.

[11] This section draws on Cohen and Kunreuther (2007).

[12] For more information on the Responsible Care program of ACC see http://www.responsiblecare-us.com/