You Can Only Die Once:
Public-Private Partnerships for Managing the Risks of Extreme Events

Geoffrey Heal
Graduate School of Business
Columbia University
New York, NY 10027
E-mail: gmh1@columbia.edu

Howard Kunreuther
Wharton School
University of Pennsylvania
Philadelphia, PA 19104
E-mail: kunreuther@wharton.upenn.edu

Visiting Research Scientist
Columbia University

March, 2002

This White Paper has been prepared for discussion at the conference "Risk Management strategies in an Uncertain World," Palisades, New York, April 12-13, 2002.

1 Introduction

There are certain bad events that can only occur once. Death is the obvious example: an individual's death is irreversible and unrepeatable. More mundane examples are bankruptcy, being struck off a professional register, and other discrete events. In addition there are other events that can in principle occur twice but that are so unlikely and/or so dreadful that one occurrence is all that can reasonably be considered. The events of 9/11/01 are perhaps of this type. A nuclear meltdown in a highly populated region is another. The fact that such events are typically probabilistic, taken together with the fact that the risk that one agent faces is often determined in part by the behavior of others, gives a unique and hitherto unnoticed structure to the incentives that agents face to reduce their exposures to these risks.

The key point is that the incentive that any agent has to invest in risk-reduction measures depends on how he expects the others to behave in this respect. If he thinks that they will not invest in security, then this reduces the incentive for him to do so. On the other hand should he believe that they will invest in security, then it may be best for him to do so too. So there may be an equilibrium where no one invests in protection, even though all would be better off if they had incurred this cost. Yet this situation does not have the structure of a prisoners' dilemma game, even though it has some similarities.

We explore this problem structure in our companion papers "Interdependent Security: The Case of Identical Agents" [Kunreuther-Heal (K-H) 2002] and "You Only Die Once: the General Case of Interdependent Security" [Heal-Kunreuther (H-K) 2002]. The fundamental question that motivates our research is: "Do organizations, such as airline companies and computer network managers, invest in security to a degree that is adequate from either a private or social perspective?" In general the answer is no. The natural next question is of course: "So what should we do about this?"

1.1 Common Features of the Problem

There are several different versions of this problem and all have certain features in common. We have already indicated one of these: a payoff that is discrete. A bad event either occurs or does not, and that is the full range of possibilities. You die or you live. A firm is bankrupt or not. A lawyer is disqualified or not. A plane crashes or not. It is not useful in these examples to differentiate the outcomes more finely.

Another feature common to the problems that we consider is that the risk faced by one agent depends on the actions taken by others – there are externalities. The risk of an airline's plane being blown up by a bomb depends on the thoroughness with which other airlines inspect bags that they transfer to this plane. The risk that a corporate divisional manager faces that his company will be sent into bankruptcy depends not only on how he manages his divisional risks but also on how other division heads behave.

Finally there is a stochastic element in all of these situations. In contrast to the standard prisoners' dilemma paradigm where the outcomes are specified with certainty, the interdependent security problem involves chance events. The question addressed is whether to invest in security when there is some probability, often a very small one, that there will be a catastrophic event that could be prevented or mitigated. The risk depends in part on the behavior of others. The unfavorable outcome is discrete in that it either happens or does not.

1.2 Importance of Problem Structure

These three factors – non-additivity of damages, dependence of risks on the actions of others, and stochasticity – are as we shall see sufficient to ensure that there can be equilibria at which there is underinvestment in risk-prevention measures. The precise degree of underinvestment depends on the nature of the problem. We focus on the two extremes that span the spectrum of possibilities. These are the security of airlines and computer networks. If an airline accepts baggage that contains a bomb, this need not damage one of its own planes: it may be transferred to another airline before it explodes. So in this framework one agent may transfer a risk fully to another. It may of course also receive a risk from another. There is a game of "pass the parcel" here. The music stops when the bomb explodes. It can only explode once so only one plane will be destroyed.

The structure of this game is quite different in the case of computer networks. Here it is commonly the case that if a virus (or hacker) enters the network through one weak point it (or he) then has relatively easy access to the rest of the network and can damage all other computers as well as the entry machine. In this case the bad outcome has a characteristic similar to a public good: its consumption is non-rivalrous. Its capacity to damage is not exhausted after it has inflicted damage once. A bomb, in contrast, has a limited capacity to inflict damage, and this capacity is exhausted after one incident.

In both cases the incentives depend on what others do. Suppose that there are a large number of agents in the system. In K-H (2002) we show that in the computer security problem, if none of the other machines are protected against viruses or hackers then the incentive for any agent to invest in protection approaches zero. For airline security, if no other airline has invested in baggage checking systems and there is a high probability that bags will be transferred from one airline to another, the expected benefits to any airline from this investment approaches 63% of what it would have been in the absence of contamination from others.

It is not only security problems that have this structure it is common to problems with discrete and interdependent risks. There are other areas where the same structure arises. Recently Arthur Anderson was sent into bankruptcy by the actions of its Houston branch. Several years ago Barings was likewise destroyed by the actions of a single trader in its Singapore branch. In each case we had multi-unit organizations in which the risk of bankruptcy faced by any unit was affected by its own choices and by the choices made by other units. In such a situation the incentive that any unit has to reduce bankruptcy risks is reduced by the knowledge that others are not doing so. A culture of risk-taking can

spread through the organization because knowledge that a few groups are taking risks reduces the incentives that others have to manage them carefully.

As we noted for the computer security problem there can be a stable equilibrium where all agents choose not to invest in risk reduction measures, even though all would be better off if they did invest. An interesting property of some of these equilibria is the possibility of *tipping* as described by Schelling (1978). How can we ensure that enough agents will invest in security that all the others will follow suit? In some cases there may be one firm occupying such a strategic position that if it changes from not investing to investing in protection, then all others will find it in their interests to do the same. And even if there is no single firm that can exert such leverage, there may be a small group. We show when this can happen and how to characterize the agents with great leverage. Obviously this finding has significant implications for policy-making. It suggests that there are some key players whom it is particularly important to persuade to manage risks carefully. Working with them may be a substitute for working with the population as a whole.

2 Characterizing the Problem: Two Agent Problem

In this section we set out formally the framework within which we study interdependent security (henceforth denoted IDS) and contrast this with other problems that have a prisoners' dilemma (henceforth PD) structure. We will utilize airline security to illustrate the IDS problem and pollution from acid rain to illustrate a PD problem

2.1 Airline Baggage Screening: An IDS Problem

Consider two identical airlines A_1 and A_2, each having to choose whether or not to invest in a baggage screening system. Each faces a risk of a bomb exploding on its plane, causing a loss of L. There are two possible ways in which damage can occur: a bomb can explode either in a bag initially checked onto the airline's own plane or in a bag transferred from the other airline. The probability of a bomb exploding in luggage initially checked on a plane of an airline that has not invested in security is p. The expected loss from this event is pL. If the airline has invested in security precautions then this risk is assumed to be zero.

Even if an airline has invested in a baggage screening system there is still an additional risk of loss due to *contamination* from the other airline if it has not invested in security. The probability of a dangerous bag being accepted for carriage by one airline and then being transferred to the other is denoted by q. The destruction of Pan Am flight 103 in 1988 was due to a bag containing a bomb that was initially checked on another airline and then transferred to Pan Am. The probability that an airline without a baggage screening system loads checked bags containing a bomb is thus $p+q$.
Assume that each airline has two choices: to invest in baggage screening, **S**, or not to do so, **N.** Table 1 shows the payoffs to the agents for the four possible outcomes:

Table 1: Expected Costs Associated with Investing and Not Investing in Security

		Airline 2 (A_2)	
		S	***N***
Airline 1 (A_1)	***S***	*Y-c, Y-c*	*Y-c-qL, Y -pL*
	N	*Y-pL, Y-c-qL*	*Y –[pL + (1-p) qL], Y –[pL+ (1-p)qL]*

Here *Y* is the income of each airline before any expenditure on security or any losses from the risks faced. The cost of investing in security is *c*. The rationale for these payoffs is straightforward. If both airlines invest in security, then each incurs a cost of *c* and faces no losses from damage so that their net incomes are *Y-c*. If A_1 invests and A_2 does not (top right entry) then A_1 incurs an investment cost of *c* and also runs the risk of a loss from damage emanating from A_2. The probability of A_2 contaminating A_1 is *q*, so that A_1's expected loss from damage originating elsewhere is *qL*. This cost represents the negative externality imposed by A_2 on A_1. In this case A_2 incurs no investment costs and faces no risk of contagion but does face the risk of damage originating at home, *pL*. The lower left payoffs are just the mirror image of these.

If neither airline invests, then both have an expected payoff of *Y- pL - (1-p)qL*. The term *pL* here reflects the risk of damage originating at ones own airline. The term *qL*, showing the expected loss from damage originating at the other airline, is multiplied by *(1-p)* to reflect the assumption that the damage can only occur once. So the risk of contagion only matters to an airline when that airline does not suffer damage originating at home.

The conditions for investing in security to be a dominant strategy are that $c<pL$ and $c<p(1-q)L$. The first constraint is exactly what one would expect if there were only a single airline: the cost of investing in security must be less than the expected loss. Adding a second airline tightens the constraint by reflecting the possibility of contagion. This possibility reduces the incentive to invest in security. Why? Because in isolation investment in security buys the airline complete freedom from risk. With the possibility of contagion it does not. Even after investment there remains a risk of damage emanating from the other airline. Investing in security buys you less when there is the possibility of contamination from others.

This solution concept is illustrated below with a numerical example. Suppose that $p= .1$, $q=.2$, $L=1000$ and c= *95*. The matrix in Table 1 is now represented as Table 2.

Table 2: Expected Costs Associated with Investing and Not Investing in Security
Illustrative Example $p = .1, q = .2, L = 1000$ and $c = 95$

		Airline 2 (A_2)	
		S	***N***
Airline 1 (A_1)	***S***	*Y-95, Y-95*	*Y-295, Y -100*
	N	*Y-100, Y-295*	*Y-280, Y- 280*

One can see that if A_2 has protection (**S**), then it is worthwhile for A_1 to also invest in security since its expected losses will be reduced by $pL = 100$ and it will only have to spend *95* on the security measure. However, if A_2 does not invest in security (**N**), then there is still a chance that A_1 will incur a loss. Hence the benefits of security to A_1 will only be $pL(1-q) = 80$ which is less than the cost of the protective measure. So A_1 will **not** want to invest in protection. In other words, either both airlines invest in security or neither of them does so. These are the two Nash equilibria for this problem.

2.2 Transboundary Pollution: A PD Problem

As a contrast to the airline security problem, consider two identical countries producing internationally mobile pollution (such as acid rain) that does not respect political boundaries. Each is harmed by its own pollution and by that released by the other country. In this case *c* is the cost of preventing pollution in a country. Pollution leads to a loss *L* with probability *p*, so that there is a stochastic element in the relationship between damage and pollution (which may for example depend on weather conditions). The loss from being polluted by activities in one's own country as well as the other country is *2pL*. In other words, losses are additive in this problem, a contrast to the IDS problem. We thus have the following payoff matrix shown in Table 3:

Table 3: Expected Payoffs to Investing and Not Investing in Pollution Prevention

		Country 2 (C_2)	
		S	***N***
Country 1 (C_1)	***S***	*Y-c, Y-c*	*Y-c-pL, Y-pL*
	N	*Y-pL, Y-c-pL*	*Y –2pL, Y –2pL*

Whenever $c < pL$ both countries will want to invest in pollution prevention. However if $c > pL$ then the dominant strategy for each country is not to invest in prevention and the expected losses to both of them will be *2pL*. Whenever $pL < c < 2pL$ it would be in the interest of both countries to invest in prevention, although they will not do so voluntarily. When this condition holds we have the structure of a PD game.

There is a key difference between the IDS and PD problems described above. In the pollution prevention problem the behavior of the other country **does not** affect the incentive to invest in pollution prevention. In the baggage security problem the behavior of the other airline **does** affect the incentive to invest in baggage security. More generally, in the pollution problem damages are additive: one country's pollution is added to that of another. More acid rain is worse than less and more greenhouse gases are worse than less. In the airline security problem, an explosion from the transfer of a contaminated bag leads to incremental losses conditional on not having a dangerous bag on your plane already. The losses are not additive. You can only die once!

To illustrate the difference between the airline security problem and the pollution prevention problem consider the illustrative example in Table 2 except that now it is certain that one is contaminated from another country if it does not invest in pollution prevention. We leave *c* unspecified and the relevant payoffs are depicted are depicted in Table 4:

Table 4: Payoffs to Investing and Not Investing in Pollution Protection
Illustrative Example $p=.1 \;\; L=1000$

		Country 2 (C_2)	
		S	***N***
Country 1 (C_1)	***S***	*Y-c, Y-c*	*Y-c-100, Y-100*
	N	*Y-100, Y-c-100*	*Y –200, Y –200*

Whenever $c > 100$ neither country will invest in pollution prevention. However if $100 < c < 200$ each would be better off if both had invested in this equipment.

2.3 Meltdown of a Nuclear Reactor: An IDS Problem

Consider now a change in the specification of this problem so that the issue is not acid rain or greenhouse gases but the meltdown of a nuclear reactor. 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 is reduced to zero. We imagine a group of small adjacent countries (e.g. Belgium, Holland and Luxembourg or Latvia, Lithuania and Estonia) so that a meltdown in any one will lead to massive radioactive contamination in all of them. Then it is reasonable to assume that the loss to any country from a meltdown is catastrophic and would not be worsened by an additional nuclear reactor accident. In this case Table 5 gives the payoffs:

Table 5: Payoffs to Investing and Not Investing in Nuclear Reactor Safeguards

		Country 2 (C_2)	
		S	***N***
Country 1 (C_1)	***S***	*Y-c, Y-c*	*Y-c-pL, Y-pL*
	N	*Y-pL, Y-c-pL*	*Y –pL-(1-p)pL, Y –pL-(1-p)pL*

Now we have a structure similar to that of the IDS problem depicted in Table 1 with *p* replacing *q* since the chances of contaminating another country are the same as the chances of contaminating one's own country. Investment in security will be a dominant strategy if $c<p\ (1-p)L$. The presence of another country that has not invested in reactor safeguards reduces the incentive to protect one's own reactor. The reason should be clear from the characterization of the problem: a meltdown elsewhere can damage a country as much as a meltdown at home. However this is only relevant if the country does not suffer a loss as a result of its own reactor's failure. By investing in protection a country reduces the risk it faces domestically but increases the chance of damage originating elsewhere from countries that have not invested in reactor safeguards.

Table 6 characterizes the outcomes for this problem for the two country case using $p=.1$ and $L=1000$ but leaving *c* unspecified so it can be contrasted with the pollution prevention case:

Table 6: Payoffs to Investing and Not Investing in Nuclear Reactor Safeguards Illustrative Example $p=.1\ \ L=1000$

		Country 2 (C_2)	
		S	***N***
Country 1 (C_1)	***S***	*Y-c, Y-c*	*Y-c-100, Y-100*
	N	*Y-100, Y-c-100*	*Y –190, Y –190*

Whenever $c < 100$ Country 1 will invest in reactor safeguards if it knows that it will **not** be contaminated by Country 2. However, if Country 2 does not invest in protection, then for Country 1 to invest in reactor safeguards it is necessary that $c< 90$. The decision rule for Country 2 is identical to that of Country 1. In contrast to the pollution prevention problem, there is a range for *c* where one country will want to invest in protective measures if the other country also does, but will not incur this cost if the other country doesn't (i.e. $100 > c > 90$). Within this range both countries will be better off by investing in protection than not investing in a manner similar to the solution of the PD problem.

3 The Multi-Agent IDS Case

We have set out our framework now for the two-agent case: this is of course the simplest and most intuitive case. The results carry over to the most general settings with some increase in complexity. In this section we review briefly the main features of the general cases, without providing detailed proofs of the results. Those can be found in [(K-H) 2002 and (H-K) 2002].

There are two key points that emerge from the discussion of the general case with respect to the IDS problem. One is that the main feature of the two-agent case carries over to n agents: the incentive that any agent faces to invest in security 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 one's own protective actions and hence reduce an agent's incentive to invest.

Secondly there is a new possibility that emerges from the multi-agent case. There is the possibility of a *tipping* phenomenon. [1] In some cases there may be one firm occupying such a strategic position that if it changes from not investing to investing in protection, then all others will find it in their interests to follow suit. And even if there is no single firm that can exert such leverage, there may be a small group. We show when this can happen and how to characterize the agents with great leverage. Obviously this point has considerable implications for policy-making: it suggests that there are some key players whom it is particularly important to persuade to manage risks carefully. Working with them may be a substitute for working with the population as a whole.

3.1 Characterization of Solutions

In the multi-agent case we can see clearly the difference between two classes of IDS problems discussed in the introduction: the airline security problem in which a bomb can damage only one airline as opposed to the virus or hacker problem, in which all agents in a computer network can be compromised by the same intruder. In this latter case, as we noted, the damage has a public good aspect to it and the capacity to inflict damage is not exhausted at the first round.

3.1.1 Airline Security

Consider first n identical airlines. Each has a probability p of loading a bomb that explodes on one of its planes if it does not invest in security systems; this probability is zero if it invests. Each also has a probability q of loading a bomb and transferring it unexploded to another airline. We assume that the probability of any one airline receiving this unexploded bomb is $q/(n-1)$. c and L give the cost of investing and the loss in the event of damage, respectively. We denote by $X(n,0)$ the total expected cost imposed on an airline which has invested in security when none of the other n-1 agents have taken

[1] See Schelling (1978) for a characterization of a number of tipping problems.

this step. In other words, $X(n,0)$ is the expected negative externality imposed on a protected airline when all the others are unprotected.[2] We show that the limit of this expression for large values of n is $(1-e^{-q})\,L$.

The externality is largest when there is only one other airline and decreases to $(1-e^{-q})L$ as the number of airlines rises. There is an obvious intuition here: as the number of airlines increases, the chance of a transferred bag reaching any particular airline falls. If there is a positive expected loss from other airlines not investing even if airline j invests itself, then its incentive to invest is reduced.

The externality is also affected by the likelihood of contamination by another airline. If $q=0$ then $X(n,0)=0$ indicating that if there are no bags transferred from one airline to another there are no negative externalities. We show that $X(n,0)$ increases monotonically in q reaching its largest value of $0.63L$ when $q=1$. If bags are transferred to other airlines with probability 1 then the expected negative externality to any airline is *63%* of the possible loss. The total expected loss to any airline is thus $[p+0.63(1-p)]L$.

3.1.2 Computer Security

When a virus infects computer j on a network, it is passed on to all other computers in the system with probability q. When none of the other $n-1$ computers invest in security then the negative externalities to a computer that has installed protection can be shown to be $X(n,0) = L$ as n gets very large.[3] In this case the expected loss to any computer j approaches L as a result of contamination from all the other unprotected computers on the network. In this situation there is no cost incentive to invest in protecting any machine against viruses or hackers.

3.2 Tipping

Now consider the tipping problem. For this it is essential that the agents differ in either their costs and/or the nature of the risks they face. We can rank firms by the total expected loss that they inflict on all others by not investing. Suppose there are n firms that can contaminate each other. If firm j changes from investing to not investing when no other firms are investing then it creates a set of negative externalities that increases the expected losses of all other firms which we denote by $E_j(n,0)$.

---

[2] We show in (K-H 2002) that

$$X(n,0) = [q/(n-1)] \sum_{t=0}^{n-2} [\,[1-q/(n-1)]^t]L = \{1-[1-q/(n-1)]^{n-1}\}\,L$$

[3] In general we show in (K-H 2002) that

$$X(n,0) = qL \sum_{t=0}^{\infty} [\,(1-q)^t] = [1-(1-q)^{n-1}]L$$

We can characterize the agents who can lead to tipping in a rather intuitive manner. We rank agents by $E_j(n,0)$. If there is a single individual who can cause all agents to invest in security, it will be the one for whom this value is largest. If tipping can be caused by a group of say K agents then this group will contain the top K agents ranked by total expected cost imposed on others by not investing.

Consider the baggage security problem. The ranking has the intuitive property that the airline that has the highest value of $E_j(n, 0)$ is the one that should be encouraged to adopt a security measure because it has the best chance of *tipping* a situation from one where no airline has adopted protection to one where every airline wants to invest in baggage security.

To be more precise, suppose that there is a Nash equilibrium at which no agent invests. Then if there is one agent *k*, with the property that if starting from this equilibrium *k* changes strategy and invests in security, then all others also do the same, then this agent must be the one for which $E_j(n,0)$ is greatest. For the other agents their best response if *k* invests in security is to also invest in security. In our companion paper H-K (2002) we give sufficient conditions for such a tipping agent and equilibrium to exist.

3.3 Societal Costs

Up until now the focus of our discussion has been on the costs of contamination to the individual agents rather than to society as a whole. From a risk management perspective one has to consider the impact that investing in security will have on the affected public.

In the airline security case the societal costs depend on three elements: (1) how many airlines invest in baggage security systems, (2) the probability (p) of a bomb being loaded onto an airline without a baggage checking system and exploding on one of its own planes and (3) the probability (q) that such a bag will be loaded and transferred to a plane from another airline before it explodes. Suppose there are n identical airlines, none of whom invest in security. Let $S(n)$ represent the societal cost when there is a loss L from any bomb explosion. For any probabilities p and q then

$$S(n) = npL + n(1-p)\{1- [1-q/(n-1)]^{n-1}\} L .$$

For the illustrative example used above where $p=.1$, $q=.2$ and $L=1000$, when $n=2$ then $S(2) = 560$. If the number of airlines increases to $n=20$, then $S(20) = 5240$.

A simple example may help to clarify the central issues in determining social costs. Suppose $p+q=1$ so that it is certain that a bomb will explode on either you own airline or another one. Let $p=q=1/2$ and assume that there are two airlines *1* and *2*. We now have four possible cases:

Case 1: Both airlines *1* and *2* load bombs that explode on their planes. In this case the loss is $2L$.

Case 2: Each airline loads a bomb and transfers it to the other airline. The loss is again $2L$.

Case 3: Airlines *1* and *2* load bombs with *1* transferring its bomb to *2* and *2* not transfer its bomb to *1*. The loss is now *L* as only airline *2* takes on a bomb that explodes.

Case 4: The reverse of *Case 2*. The loss is *L* as only airline 1 takes on a bomb that explodes.

Since each of these four cases has an equal chance of occurring the expected social loss is *1.5L*.

Turning to the computer security problem, the societal losses depend on the number of computers *n* in the network. Define *S(n)* as the societal cost if none of the computers have security systems. Then for any probabilities *p* and *q:*

$$S(n) = npL + n(1-p)\{1-(1-q)^{n-1}\}L$$

For the illustrative example where *p=.1, q=.2* and *L=1000* for n=2 *S(2) =280*. As n gets larger, then *S(n)* approaches *nL=1000n.* If there are enough computers on any network it is almost certain that each machine will experience a loss.

Turning now to typical prisoner's dilemma (PD) problems, the damage from others is normally assumed to be additive. Hence if we have *n* countries each of whom pollutes with probability *p* then the expected negative externalities (i.e. pollution damage from others) to any country is *(n-1)pL* . The larger the number of countries polluting, the more serious is the resulting damage to individual countries. The expected pollution impacts at the global level are *npL*. Furthermore in a PD problem an increase in the number of agents does not affect the incentive that any one has to stop polluting. If *n=20, p=.1* and *L=1000* then the expected global pollution loss is 2000.

Note that the expected societal cost for IDS problems is larger than for PD problems for the same parameters, simply because the chances that any agent will suffer a loss is greater than *p* because of the possibility of contamination from others. (i.e. q>0). For computer network-like problems this probability approaches 1 as *n* gets large. Hence there is a strong need for developing risk management strategies for reducing these costs.

4 Proposed Risk Management Solutions to the IDS Problem

How can we overcome the impact of contamination on an agent's investments in security? Below we examine a set of different measures ranging from private market mechanisms to regulations to collective choice that may internalize the externalities associated with protective measures where there are interdependencies between agents. We use the airline security problem to illustrate the role of different policy tools but they apply to any IDS problem.

4.1 Insurance

Insurance appears to be a logical way of encouraging security since it rewards those who adopt protective measures by reducing their premium to reflect the lower risk. However,

in order to deal with the externalities created by others who do not invest in protection, the agent causing the damage must be forced to pay for the losses. For example, if a bag transferred from Airline 1 to Airline 2 exploded, Airline 1's insurer would have to pay for the cost of the damage to Airline 2. This is not how current insurance practice operates. An insurer who provides protection to A_i is responsible for losses incurred by agent i no matter who caused them.[4] One reason for this contractual arrangement between the insurer and insured is the difficulty in assigning causality for a particular event.[5]

Interestingly enough social insurance programs have the advantage over a competitive insurance market in encouraging investment in security. If the government were to insure all the airlines then it would want to internalize the externalities associated with contaminated baggage transferred between airlines. Each airline investing in a screening system would be given premium reductions not only for the reduced losses to its own planes but also for the reduction in losses to all the others. Under such a program as long as $c < pL$, there would be an incentive for all airlines to invest in baggage security.

4.2 Liability

If an airline that caused damage to other airlines by not adopting a protective measure were held liable for these losses, then the legal system would offer another way to internalize the externalities due to IDS. However we know of no cases in which an agent has been held liable for the damages to others because it did **not** invest in protection. In the case of an aircraft explosion, it would be difficult to know whether a bag from another airline was the cause or whether it was one of the airline's own bags. The Pan Am crash in 1988 illustrates this difficulty. The bag that destroyed the plane was in a container of transferred bags and it took considerable detective work to determine which one actually caused the crash.

4.3 Taxation

A more direct way of encouraging greater security is to levy a tax of t dollars on any airline that does not invest in baggage security. The magnitude of the tax depends on the number of agents and the cost of protection, c. In K-H (2002) we have shown that for identical airlines, any firm will want to invest in protection when no one else does, if the tax t is greater than $c - p[L - X(n,0)]$. This implies that as the negative externalities $[X(n,0)]$ increase, the tax also increases.[6] Note that a subsidy on protective measures plays an identical role in inducing agents to invest in security. The cost c is reduced due to the subsidy, so that the protective measure is more attractive to the agent.

---

[4] If the damage from an insured risk is due to negligence or intentional behavior then there are normally clauses in the insurance policy that indicate that losses are not covered (e.g. a fire caused by arson).

[5] With respect to fire damage a classic case is H.R. Moch Co., Inc. v Rensselaer Water Co. 247N.Y.160, 159 N.E. 896 which ruled that "A wrongdoer who by negligence sets fire to a building is liable in damages to the owner where the fire has its origin, but not to other owners who are injured when it spreads". We are indebted to Victor Goldberg who provided us with this case.

[6] Note that if $c \leq p(L - X(n,0))$ then there is no need to impose any tax on an agent for it to want to invest in protection on its own because the internal benefits from protection exceed the cost of protection even if the airline faces negative externalities from transferred bags.

4.4 Regulations and Standards

The possibility of contamination by other units provides a rationale for well-enforced regulations and standards requiring individuals and firms to adopt protective mechanisms. The need for baggage review systems took on greater importance after the Sept. 11th tragedies and has led the government to require their use by the airlines. The U.S. Congress now requires airlines to have a checked baggage security program to screen all bags for bombs (NY Times 2002).

4.5 Coordinating Mechanisms

One way to convince the *n* independent airlines that it would be in everyone's best interests to invest in protection is to utilize some official organization to coordinate these decisions. For example, the International Air Transport Association (IATA), the official airline association, has indicated on its Web site that since Sept. 11th they "have intensified hand and checked baggage processing". IATA could have made the case to all the airlines that they would be better off if each one of them utilized internal baggage checking, so that the government would not have had to require this.

An association can play a coordinating role by stipulating that any member has to follow certain rules and regulations, including the adoption of security measures. A member has the right to refuse to do business with any non-member or an agent that has not subscribed to the ruling. IATA could require all bags to be reviewed carefully and each airline could indicate that it would not accept in-transit bags from airlines that did not adhere to this regulation.

IATA follows this type of policy in agreements regarding pricing policies. If an airline does *not* belong to IATA and you want to transfer to this airline from an originating IATA airline, the originating airline will not make a reservation for you. Furthermore an IATA airline will not honor a non-IATA airline ticket unless it conforms to the IATA tariff conference (e.g. US Air will not honor a JetBlue airline ticket).[7]

5 Extending the Analysis

The choice of whether to protect against events where there is interdependence between your actions and those of others raises a number of interesting theoretical and empirical questions. We mention some of these in this section.

5.1 Differential Costs and Risks

The nature of stable Nash equilibria for the problems considered above and the types of policy recommendations may change as one introduces differential costs across the agents who are considering whether or not to invest in security.

[7] See the IATA web site at http://www.iata.org/membership/steps.asp#10

Consider each airline deciding whether to invest in a baggage security system. In H-K (2002) we have shown that if there are differential costs and/or risks between companies, we would expect to find some airlines investing in baggage security systems and others who would not. Furthermore, as we discussed above, the airline which creates the largest negative externalities for others should be encouraged to invest in protective behavior not only to reduce these losses but also to induce other airlines to follow suit thus inducing *tipping* behavior.

5.2 Multi-Period and Dynamic Models

Deciding whether to invest in security normally involves multi-period considerations since there is an upfront investment cost that needs to be compared with the benefits over the life of the protective measure. An airline that invests in a baggage security system knows that this measure promises to offer benefits for a number of years. Hence one needs to discount these positive returns by an appropriate interest rate and specify the relevant time interval in determining whether or not to invest in these actions. There may be some uncertainty with respect to both of these parameters.

From the point of view of dynamics, the decision to invest depends on how many others have taken similar actions. How do you get the process of investing in security started? Should one subsidize or provide extra benefits to those willing to be innovators in this regard to encourage others to take similar actions?

5.3 Behavioral Considerations

The models discussed above all assumed that individuals made their decisions by comparing their expected benefits with and without protection to the costs of investing in security. This is a rational model of behavior. There is a growing literature in behavioral economics that suggests that individuals make choices in ways that differ from the rational model of choice. (Kaheman and Tversky 2000).

With respect to protective measures there is evidence from controlled field studies and laboratory experiments that many individuals are not willing to invest in security for a number of reasons that include myopia, high discount rates and budget constraints. (Kunreuther, Onculer and Slovic 2000). In the models considered above there were also no internal positive effects associated with protective measures. Many individuals invest in security to relieve anxiety and worry about what they perceive might happen to them or to others so as to gain peace of mind (Baron, Hershey and Kunreuther 2000). [8]

A more realistic model of interdependent security that incorporated these behavioral factors as well as people's misperceptions of the risk may suggest a different set of policy

[8] Of course, if these individuals become aware that substantial losses may be imposed on them or their firm from others who are unprotected, then this new knowledge may increase their anxiety by showing that investing in these protective measures has more limited benefits than they had initially assumed it would.

recommendations than a rational model of choice. For example, if agents were reluctant to invest in protection because they were myopic, then some type of loan may enable them to discern the long-term benefits of the protective measure. A long-term loan would also help relieve budget constraints that may deter some individuals or firms from incurring the upfront costs of the risk-reducing measure.

6 Future Research on Risk Management Strategies for IDS Problems

We conclude by suggesting a set of problems that involve interdependent security and suggesting the types of risk management strategies that could be explored for addressing them.

6.1 Types of Problems

The common features of IDS problems are the possibility that other agents can contaminate you and your inability to reduce this type of contagion through investing in security. You are thus discouraged from adopting protective measures when you know others have decided not to take this step. Here are some problems that fit into this category, some of which have been discussed in this paper:

- Investing in airline security
- Protecting against chemical and nuclear reactor accidents
- Making buildings more secure against attacks
- Investing in sprinkler systems to reduce the chance of a fire in ones apartment
- Avoiding gambles by divisions in a firm that could bring the entire firm into bankruptcy .Two recent examples come to mind: (1) Nick Leeson operating in the Singapore futures market division causing the collapse of Baring's Bank and (2) Arthur Anderson being brought into bankruptcy by the actions of its Houston branch.
- Making computer systems more secure against terrorist attacks.
- Investing in protective measures for each part of an interconnected infrastructure system so that services can be provided to disaster victims after the next earthquake.

In each of these examples there are incentives for individual units or agents not to take protective measures but there are large potential losses to the organization and to society. Furthermore the losses are sufficiently high that they are non-additive. An airplane can only be destroyed once; a building can only collapse once; one can only be bankrupt once; an interconnected system is only as good as its weakest link. You can only die once!

IDS problems can be contrasted with other types of protective measures that do **not** have these features. Two that are discussed in more detail in K-H (2002) are theft protection and vaccination. In the case of theft protection if you install an alarm system that you announce publicly with a sign, the burglar will look for greener pastures to invade. With respect to vaccines if you knew everyone else has been vaccinated, then there would be no point in getting vaccinated since you cannot catch the disease.

6.2 Risk Management Strategies

For each IDS problem there are a range of risk management strategies that can be pursued by the private and public sectors for encouraging agents to invest in cost-effective protective measures.

- Collecting information on the risk and costs (e.g. constructing scenario so that one can estimate p, q, L and c with greater accuracy).

- Designing incentive systems (e.g. subsidies or taxes) to encourage investment by agents in protective measures.

- Developing insurance programs for encouraging investment in protective measures when firms are faced with contamination.

- Structuring the liability system to deal with the contamination effects of IDS

- Carefully designed standards (e.g. building codes for high-rises to withstand future terrorist attacks) that are well-enforced through mechanisms such as third-party inspections.

- Introducing federal reinsurance or state-operated pools to provide protection against future losses from terrorist attacks to supplement private terrorist insurance

It may be desirable to integrate several of these measures through public-private risk management partnerships. For example, banks and financial institutions could require that firms adopt security measures as a condition for a loan or mortgage. To ensure that these measures are adopted there may be a need for third party inspections or audits by the private sector. Firms who reduce their risks can be rewarded through lower insurance premiums. If there are federal or state reinsurance pools at a reasonable prices to cover large losses from a future terrorist attack then private insurers may be willing to provide terrorist coverage at affordable premiums

6.3 Questions for Discussion

In undertaking future research on interdependent security issues here are some broad questions that could be addressed:

- How can new technologies (e.g. identification and tracking protocols) aid in the detection of suspects and serve as effective communication devices and preventive measures?

- What is the recommended balance between government and private sector risk sharing and cost sharing for different security measures?
- What types of public-private partnerships are needed (in the short-run and long-run) to provide insurance and other forms of financial protection?

- What types of strategies should be developed to encourage adoption of protective measures (e.g. insurance, liability regulations, taxation, subsidies, coordinating mechanisms such as professional associations)

SELECTED REFERENCES

Arthur, Brian (1994) *Increasing Returns and Path Dependence in the Economy*. Ann Arbor: University of Michigan Press.

Ayres, Ian and Steven Levitt (1998) "Measuring the Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack" *Quarterly Journal of Economics* 113: 43-77.

Baron, Jonathan., Hershey, John and Kunreuther, Howard. (2000). Determinants of priority for risk reduction: the role of worry. *Risk Analysis, 20*, 413-427.

Cohen, Linda and Noll, Roger (1981) "The Economics of Building Codes to Resist Seismic Shocks" *Public Policy* Winter 1-29.

Cummins, J. David, Doherty, Neil and Lo, Anita. (2002). "Can Insurers Pay for the 'Big One?' Measuring the Capacity of an Insurance Market to Respond to Catastrophic Losses." *Journal of Banking and Finance* (in press)

Cummins, J. David and Doherty, Neil (2002) "Federal Terrorism Reinsurance: An Analysis of Issues and Program Design Alternatives" Paper Presented at the NBER Insurance Project Workshop, Cambridge Mass. Feb. 1.

Freeman, Paul K, and Kunreuther, Howard (1997). *Managing Environmental Risk Through Insurance* (Boston: Kluwer; Washington, DC: American Enterprise Institute).

Froot, Kenneth. (ed) (1999). *The Financing of Property/Casualty Risks*, Chicago: University of Chicago Press.

General Accounting Office (GAO) (2001) "Terrorism Insurance: Alternative Programs for Protecting Insurance Consumers" Testimony of Thomas McCool Before the Committee on Banking, Housing and Urban Affairs, US Senate. October 24.

General Accounting Office (GAO) (2002.) "Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities" Testimony of Richard J. Hillman Before the Subcommittee on Oversight and Investigations, Committee on Financial Services, House of Representatives. February 27.

Gollier, Christian (2000) "Towards an economic theory of the limits of insurability", *Assurances* January, pp.453-474.

Heal, Geoffrey (1994). "Formation of International Environmental Agreements," in C. Carraro (ed.) *The International Dimension of Environmental Policy*, Boston: Kluwer.

Heal, Geoffery (1999a) "Price and Market Share Dynamics in Network Industries". Chapter 10 of G. Chichilnisky (ed) *Markets, Information and Uncertainty: Essays in Honor of Kenneth J. Arrow.* New York: Cambridge University Press.

Heal, Geoffrey (1999b) “New Strategies for the Provision of Global Public Goods: Learning from international environmental challenges.” in I Kaul and M. Stern (ed) *Global Public Goods* New York: Cambridge University Press.

Heal, Geoffrey and Kunreuther, Howard (2002) “You Only Die Once: the General Case of Interdependent Security” (mimeo)

Hershey John, Asch D, Thumasathit T, Meszaros J, and Waters V, (1994) "The Roles of Altruism, Free Riding, and Bandwagoning in Vaccination Decisions," *Organizational Behavior and Human Decision Processes* 59:177-187.

Jaffee, Dwight and Russell Thomas (2002) “Extreme Events and the Market for Terrorism Insurance: Paper Presented at the NBER Insurance Project Workshop, Cambridge Mass. Feb. 1.

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

Kleindorfer, Paul and Kunreuther, Howard. (1999). “The Complementary Roles Of Mitigation And Insurance In Managing Catastrophic Risks." *Risk Analysis*, 19:727-38.

Kunreuther, Howard and Heal, Geoffrey (2002) “Interdependent Security: The Case of Identical Agents” Wharton Risk Management and Decision Processes Center Working Paper Philadelphia: University of Pennsylvania

Kunreuther, Howard (2002) “The Role of Insurance in Managing Extreme Events: Implications for Terrorist Insurance *Business Economic* April.

Kunreuther, Howard, Onculer, Ayse and Slovic Paul (1998) “Time Insensitivity for Protective Measures” *Journal of Risk and Uncertainty*, 16: 279-299.

NY Times (2002) “Airlines Scramble to Meet New Bag Check Deadline” January 14.

Orszag, Peter and Stiglitz, Joseph (2002) “Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities” January (mimeo).

Ostrom, Elinor. (1990) *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge, UK: Cambridge University Press.

Philipson, Tomas (2001) “Economic Epidemiology and Infectious Diseases” in Joseph Newhouse and Anthony Culyer eds *The Handbook of Health Economics* North Holland Press.

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

Sunstein, Cass (1996) "Social Norms and Social Roles," *Columbia Law Review* 96:903-68.

Swiss Re (2002) *Terrorism—dealing with the new spectre"* Zurich: Swiss Re Feb.