



Risk Management and Decision Processes Center

“Interdependent Security and Managing Extreme Events”

Report on a Roundtable held by the Wharton Risk Management and Decision Processes Center, in conjunction with the Earth Institute at Columbia University, on January 30, 2004 in Philadelphia. The center is co-chaired by Paul Kleindorfer and Howard Kunreuther

EXECUTIVE SUMMARY

The interdependent nature of security risks presents a unique challenge in the age of global terrorism. Risk-management strategies, such as enhanced security measures or terrorist insurance policies, can only be effective if all entities in a given operating system are adequately protected. The decision by an airline, for example, to screen every item of luggage on every flight will be compromised if other airlines whose flights connect with it do not also follow the same rigorous procedure. Similarly, the collapse of the World Trade Center on Sept. 11, 2001 could be attributed in part to the failure of security at Logan airport in Boston to prevent some of the terrorists from boarding the planes that flew into the twin towers.

Recognition of the vulnerability of one part of a system to weaknesses elsewhere can act as a disincentive for individual components to improve their own operations. Effective risk management strategies will require the development of public-private partnerships tasked with improving data, providing incentives, issuing regulations, and providing adequate compensation thru insurance or reinsurance against extreme events such as a terrorist attack. In this connection the Terrorist Risk Insurance Act of November 2002 has guaranteed the availability of terrorism insurance to commercial enterprises but there is currently limited interest in purchase. Rates in January 2004 were similar to those in April 2003, indicating there has been no increase in the perceived risk by insurers.

All parties seeking to manage terrorist risk continue to be hampered by the difficulty of estimating the likelihood and nature of an attack. Officials within the Department of Homeland Security (DHS) are operating on the basis of “not if but when” another terrorist attack occurs. The expectation that another attack will be catastrophic is increased by the belief that terrorists will seek to gain the maximum impact from their limited resources.

Modelers accumulate data and simulate the circumstances of possible terrorist attacks via the construction of scenarios for a range of institutions including the electric power generating industry, the U.S. navy, and for major ports. They are challenged by the need to obtain high-quality information, such as the number of people working in a particular building in the course of assessing risk. Insurers typically use the models to gauge their proximity to targets, identify large losses and aggregate their risk. There is a need for better information on indirect losses such as business interruption stemming from extreme events.

Though there has been increased interest since 9/11 in assessing and managing extreme events, there is a need for the private sector to be more proactive in the development and implementation of risk-management strategies, rather than waiting for government requirements or incentives. Strategies should integrate enhanced physical and cyber security as a core element of the corporate culture.

Future research needs include:

- ◆ Shoring up the weakest link
- ◆ Identifying sources of interdependence
- ◆ Modeling the risks
- ◆ Evaluating indirect losses such as business interruption
- ◆ Alternative risk-sharing mechanisms as well as international comparisons
- ◆ Behavioral research on decision processes and choice
- ◆ Understanding institutional arrangements for specific problem contexts
- ◆ Public-private cooperation in the United States and abroad

A list of participants in the Roundtable with their e-mail addresses can be found at the end of the Report.

REPORT:

1. Interdependent Security and Terrorism Risk

When the fates of many companies are intertwined, their incentives to attend to security issues can be severely reduced- Kunreuther, Heal and Orszag, Brookings Institution Policy Brief, October 2002

Government intervention may be required when companies are deterred from making appropriate security investments by the knowledge that others in their system have failed to do so.

Geoffrey Heal of Columbia University illustrated how “weak links” outside of the U.S. potentially compromise the security of U.S. public health, the power grid, and airlines based on interdependence. “If you wanted to bomb a U.S. airline, you wouldn’t put the bomb on a U.S. carrier in the first place,” he said, with reference to Pan Am flight 103 in which a bomb exploded that had been loaded on a connecting flight in Malta and then transferred, via Frankfurt and London to the Pan Am plane that exploded over Scotland in December 1988. South China is the weakest part of the system for both airline security and public health, while Canada represents the greatest vulnerability of the U.S. electric power grid, Heal said.

The cooperation of overseas regulators is vital in this effort because “system boundaries do not coincide with national boundaries.” Regulators should rely on a very broad interpretation of the systems they are working on by aiming to identify and prevent potential weak links.

Regulators should also consider the impact of current privacy laws. Heal noted that Richard Reid, the British citizen who smuggled a “shoe bomb” onto a flight from Paris to Miami, was able to board the flight because his criminal record was not available to French and U.S. officials under United Kingdom privacy law. Heal pointed out that the information pertinent to security could be provided voluntarily and is most likely not central to the concerns of privacy advocates.

Recognizing interdependent risk is a challenge for the insurance industry seeking to cover one part of a complex system. Even sophisticated risk management can be compromised by invisible failures elsewhere in the system. “Insurability requires minimum comfort levels with the system as a whole,” Heal said in his presentation.

A risk-management strategy should be based on a number of elements within an interdependent security framework, Howard Kunreuther of the University of Pennsylvania told the conference. A risk assessment and vulnerability analysis will contribute to a modeling of risks and statistical data building scenarios. Strategies should also account for corporate and public perceptions of risk. Plans may consist of a number of risk-management tools including incentives such as fines, regulation, compensation and insurance. Evaluation processes should address both the impacts on the different interested parties and on society in general.

Public and corporate perception of the risk of terrorism has declined since the aftermath of Sept. 11, 2001, Kunreuther said. In the immediate wake of that catastrophic event, businesses in New York City and other highly populated areas were willing to purchase insurance at high premiums but could not obtain coverage. With no attacks on the U.S. mainland in the past 27 months, there has been limited interest in terrorism insurance because of a perception that “It won’t happen to me.” There has been a failure to think about the economic consequences of being unprotected and hence a reluctance to invest

in protective measures. This lack of interest in mitigation has been exacerbated by myopia on the part of decision-makers who want quick returns on their investments.

The complexity of interdependent risk coupled with misperceptions of the risk suggests the need for government working with the private sector to manage it. Such cooperation could include constructing attack scenarios, designing incentives such as fines or subsidies to encourage investment in security, designing insurance programs and well-enforced regulations that are cost-effective.

Mel Bernstein of the Department of Homeland Security (DHS) described the agency's research agenda, which includes investigating countermeasures for biological, chemical, radiological and nuclear attacks as well as threat and vulnerability testing and assessment. A key question facing the division is how to prioritize DHS initiatives.

DHS assumes there will be another attack on the U.S., Bernstein said. "People say not if there will be a terrorist event but when there will be a terrorist event." The division aims to encourage scientific and technological advances that analyze new and emerging threats; to establish and expand national systems to benefit public and private bodies, and to influence the national research agenda for countering threats from CBRN and conventional attacks.

Todd Sandler of the University of Southern California highlighted the value of game theory in analyzing the terrorist threat. Game theory is more useful for looking at terrorism than for natural disasters because terrorism has the human element. Sandler called for a model that represents a spectrum of risk based on the idea of the "weaker link" in which the smallest effort determines the safety of the entire system. For example, if transferred airline baggage isn't checked after transfer, then the least-vigilant check determines everyone's safety.

Sandler drew a distinction between offensive and defensive measures in the war on terror and argued that most of the spending so far has been on offensive measures –the wars in Iraq and Afghanistan. Other countries have been "free riding" on America's anti-terrorist efforts. He recommended careful analysis of the allocation of resources for protective measures among alternative potential targets, and identified current vulnerabilities related to surface-to-air missiles, containers entering via ports, as well as biological attacks on cities.

Sandler also argued that the U.S. needs a better system of discerning specific threats, and said there should be less reliance on the "chatter system" which intercepts terrorist communications, and can be manipulated by them.

2. Insuring Against Terrorism and other Extreme Events

In evaluating risk, the insurance industry is doing a better job of accumulating exposure data such as the number of employees on the payroll at the insured's location, said John DeMartini of Towers Perrin. The marketplace expects submissions to include high-quality, detailed exposure information such as construction codes, the age of a building, and its occupancy. That information is widely available because it is used for natural catastrophe modeling. Brokers working with insurers and reinsurers have a role to play in education, analysis, market knowledge, negotiation, and attention to detail.

The perception of risk among insurers and reinsurers does not appear to have changed significantly in the last nine months, DeMartini said. He cited the example of a Midwest mutual insurance company providing coverage to small and medium-sized commercial businesses. The reinsurer recently provided the insurer with up to \$70 million worth of protection if terrorism losses exceeded \$15 million at a pre-

mium of \$6.75 million. The resulting rate was essentially the same as the 10 percent rate that DeMartini cited in an example at the last Extreme Events Roundtable in April 2003. In that case, up to \$9 million in terrorism coverage was provided for losses exceeding \$1 million and cost the insurer \$900,000.

But obtaining reinsurance can be a challenge. DeMartini cited the case of an East Coast mutual insurance company writing personal and small commercial business that was unable to obtain terrorism coverage from London reinsurers for business in 11 major U.S. cities. In helping clients manage extreme events, brokers are challenged by the standards of rating agencies, he said. The standards lack clarity, standard methodology and standard benchmarks.

The changing nature of the available models creates an additional challenge for brokers advising their clients about terrorism coverage. The models are evolving in response to new information about terrorist groups, attack modes and weaponry and create an extra level of uncertainty among companies trying to manage risk.

DeMartini suggested that reinsurers might be unable to meet the losses from another attack of the magnitude of Sept. 11, 2001, and so might simply leave the market in response to the next catastrophic event.

For insurers, a major question is whether the Terrorist Risk Insurance Act (TRIA) will be extended beyond its current expiration in 2005 and if so, under which conditions. Jim Macdonald of ACE USA asked whether the market would return to the strict rationing of insurance cover in major cities that occurred in the months before TRIA's enactment in November 2002.

TRIA has been of vital importance in providing stability to the property and casualty insurers in markets perceived as having the highest risk. Still, there is no efficient reinsurance market for the highest risks and almost no reinsurance capacity for chemical, biological, radiological and nuclear (CBRN) attacks. When TRIA does eventually expire, the industry will need to agree on acceptable levels of preparedness and benchmarks for prudent care that will encourage insurance capital to underwrite high-risk accounts, Macdonald said.

Insurance rating agencies are faced with the challenge of assessing exposure now that data is being required at the level of individual buildings. "Will the agencies and regulators set standards for an acceptable level of exposure for an insurer,?" Macdonald asked.

In major cities, already perceived as the highest-risk areas, risk is being increased by the fact that skyscrapers are still being built, said Christopher Yaure of Employers Reinsurance Corp.

In the context of the World Trade Center disaster, Yaure highlighted the reinsurance risks associated with extreme events. They include large losses, inadequate data and rapidly changing risk assessments as more data are accumulated on people and property to be insured. The challenges to reinsurers in deciding whether to share the risk from extreme events include multiple insurers, multiple insureds, and large geographic areas to be covered.

3. Interdependent Security and Enterprise Risk Management (ERM)

Companies seeking to manage extreme event risk are making significant changes including the integration of ERM risks across the entire organization and the identification and management of new risk classes that may not have been present before 9/11. Changes are occurring in nearly every sector of business and government. In the private sector, the new approach is driven by the vision of integrating

the management of security with other major risks facing a company, Paul Kleindorfer of the University of Pennsylvania told the conference. The process includes assignment of responsibility for ERM by each unit of the firm and their undertaking a vulnerability assessment, a risk analysis and a cost-benefit analysis.

At Wachovia, a firm with some 10,000 locations and 83,000 employees, ERM is being fully integrated with the company's daily business, "Security and risk management is not something that you can bolt on," said Tom Gallagher of Wachovia Securities. "Everybody has to own it, and it takes a long time to trickle down through 83,000 people."

Wachovia sees decentralization as a part of its risk management strategy. For example, the fact that it isn't based in lower Manhattan allowed it to keep operating immediately following the 9/11 attacks. Similarly, any two of the company's four trading rooms around the world can pick up the slack if the others go down, Gallagher said. But ERM is a challenging project for a company that is the result of some 80 mergers and where different cultures have to work toward the same goal. Different divisions with different philosophies manage physical security and cyber security.

ERM provides a competitive advantage when done appropriately because it will attract investors and employees who believe the company has the right systems in place to resist terrorist attack on a physical or cyber level. A successfully implemented ERM program may also help to prevent terrorist attacks because it will deter perpetrators who see that they cannot disrupt business to any great extent.

Studies of cases, such as Wachovia, would be a useful tool for others, said David Durbin of Swiss Re. Such studies should include data on how the program has affected the share price and the company's reputation in the industry. Durbin called for the adoption of a common language of risk management so that standards can be drawn up and benchmarks set.

In an effort to understand the whole process of interdependent risk, Durbin said researchers should compile case studies on companies that have embraced ERM. The studies should also look at the impact of ERM on a company's share price and its reputation in the industry.

Standard terminology is also needed for risk assessment, said Irv Rosenthal, of the Wharton Risk Center. Differences in risk-assessment methodology and terminology can lead to a failure to recognize weaknesses in organizational units that could compromise the security of the whole.

Although concepts such as vulnerability, threats and security have entered the national discussion on risk, there are no commonly accepted definitions of such terms as "adequate" security or "credible" threats, Rosenthal said. He urged companies to agree on an operational definition of "safety" which should take into account the enterprise's culture and special needs as well as the standard requirements of law and customs.

4. The role of modeling in dealing with interdependent risks

Those who simulate the risk of terrorism and other extreme events by building models are confronted with a series of challenges. They include obtaining high-quality information, adjusting the model to allow for new information, and influencing the dynamics of the insurance and reinsurance markets.

"Modeling recognizes the international interdependency of both the threat from Islamist militants and the actions of counter-terrorism agencies," said Gordon Woo of Risk Management Solutions. "An illustration of the global nature of the terrorist threat is that the toxin ricin was found in an area of London

known as *Little Algeria*,” Woo said. As a sign of the need for governments to act in concert against the terrorist threat, he cited the case of Rachid Ramda, the financier of the 1995 Paris metro bombing campaign, who was given asylum in Britain, a decision that was only rescinded after 9/11.

Another modeling firm, Applied Insurance Research (AIR), aims to obtain a more complete picture of those extreme events that could have a noticeable negative impact on the financial results of insurance companies, said Jack Seaquist of AIR Worldwide. The model establishes underwriting guidelines and policy pricing for viable terrorism coverage. As a result, insurance companies can analyze their own exposure, determine their proximity to targets, identify large losses, and aggregate their risk. Such analysis is possible because AIR possesses an extensive database containing data on locations, values, construction and occupancy, covering commercial and residential property, workers, residents, mobile homes and automobiles.

Dennis Kuzak of EQECAT pointed out that his firm conducts scenario-based risk assessments using data from agencies including the U.S. Coast Guard, the Center for Chemical Process Safety, and the Electric Power Research Institute. In constructing probabilistic risk models, the company incorporates target sites, initiating events, event footprints and a vulnerability assessment.

5. The University of Southern California DHS Research Center

Further study of terrorism risk is being conducted by the Department of Homeland Security’s Research Center at the University of Southern California (USC) with the cooperation of other universities in the United States. Its focus is the analysis of risks and the economic consequences of terrorism, said Detlof von Winterfeldt of USC, one of the Center’s co-directors.

The Center is creating models on infrastructure; chemical, biological and radiological attacks, and agriculture. Its principal challenges include assessing the probability of attack, allocating budgets in the context of the political environment, determining the appropriate level of security, and trading off security benefits with social costs such as an erosion of privacy.

Despite nationwide preparation for future terrorist attack, there is still a risk of surprise, von Winterfeldt said. “My guess would be that the next event that happens will be something we have not thought of.”

6. Areas for Future Research

Four areas were identified as potential case studies: the airline industry, the power grid, the chemical industry and terrorism insurance coverage. Within these cases, there are a range of issues to be studied. They include:

- Shoring up the weakest link
- Identifying sources of interdependence
- Modeling the risks
- Evaluating indirect losses such as business interruption
- Alternative risk-sharing mechanisms as well as international comparisons
- Behavioral research on decision processes and choice
- Understanding institutional arrangements for specific problem contexts
- Public-private cooperation in the United States and abroad

An **airline industry** study should focus on further applications of a 2003 study by the Wharton Risk Center that looked at a data set of 32,000 anonymous civilian flight itineraries including airports, carriers and transfers. This new and larger study should identify strategically important airlines that would become pioneers for the rest of the industry in enhancing risk management.

For the **power grid**, the focus should be on independent investment under distributed ownership. The main challenge for this study would be that the industry is nowhere near a steady state, and already suffers from under-investment before the additional burden of security concerns are added. Last summer's blackouts in the Northeast, Canada and Italy are a vivid illustration of this. An additional challenge for the power industry study would be that the industry has many regulators, all of whom are interdependent.

In the **chemical industry**, the proposed study should focus on integrating security assessment and management with insurance and ERM systems. The main challenge is that the industry faces significant competitive pressures, and so is reluctant to make additional investment in security.

The proposed study on **terrorism insurance** should look at how well foreign solutions are working in practice in European countries and whether some features would be more appropriate when TRIA ends in 2005. This study should compare issues, such as eligibility for coverage, pricing under terrorism coverage, how insurers and reinsurers are sharing the risk, whether the public sector is taking on any of the risk, and whether the government has an exit strategy.

The Wharton Risk Center is now undertaking a study for the Organization for Economic Cooperation and Development (OECD) Task Force on terrorism insurance established in 2002 and have held meetings with the U.S Treasury and the principal stakeholders of the French and German terrorism insurance programs. A study on terrorism insurance and TRIA was published at the end of 2003 by the Wharton Risk Center. In January a Risk Center Working Paper compared terrorism insurance in France, Germany and the United States.

The Wharton Risk Center looks forward to working with its industry sponsors, public sector agencies and the University of Southern California DHS Research Center on linking risk assessment, risk perception and risk management for dealing with the challenges of extreme events. In particular, there is a need for understanding the decision processes and institutional arrangements that characterize terrorism and other potential catastrophic risks where there are interdependencies between different interested parties. Researchers and practitioners can then work together in developing creative public-private partnerships for managing these extreme events in a more effective and equitable manner than under current programs.

**Wharton Risk Management & Decision Processes Center
January 30, 2004 Extreme Events Meeting
Attendee List**

Name	Company	Email
Ralph Ahn	Wharton School, Univ. of Penn	ahnr@wharton.upenn.edu
Debra Ballen	American Insurance Association	dballen@aiadc.org
Samira Barakat	Employers Reinsurance	Samira.Barakat@ercgroup.com
Melvin Bernstein	U.S. Department of Homeland Security	melvin.bernstein@dhs.gov
Vicki Bier	University of Wisconsin	bier@ie.engr.wisc.edu
John DeMartini	Towers Perrin Reinsurance	demartj@towers.com
Robin Dillon	Georgetown University	rld9@georgetown.edu
Lloyd Dixon	RAND	dixon@smail1.rand.org
Neil Doherty	Wharton School, Univ. of Penn	doherty@wharton.upenn.edu
Emily Donovan	Lockheed Martin Integrated Systems & Solutions	emily.h.donovan@lmco.com
David Durbin	Swiss Reinsurance Company	David_Durbin@swissre.com
Walter Enders	University of Alabama	wenders@cba.ua.edu
Deanna Fidler	Employers Reinsurance Corporation	Deanna.Fidler@ercgroup.com
Richard C. Franklin	ACE INA	rich.franklin@ace-ina.com
Tom Gallagher	Wachovia Securities	tom.gallagher@wachovia.com
Geoffrey Heal	Columbia University	gmh1@columbia.edu
Ken Jenkins	American Re-Insurance Company	kjenkins@amre.com
Paul Kleindorfer	Wharton School, Univ. of Pennsylvania	kleindorfer@wharton.upenn.edu
Howard Kunreuther	Wharton School, Univ. of Pennsylvania	kunreuther@wharton.upenn.edu
Dennis Kuzak	EQECAT, Inc.	dek@eqe.com
Jim Macdonald	ACE USA	james.macdonald@ace-ina.com
Don Mango	Employers Reinsurance	don.mango@ercgroup.com
Robert Meyer	Wharton School, Univ. of Pennsylvania	meyerr@wharton.upenn.edu
Erwann Michel-Kerjan	Wharton Risk Center	erwanmk@wharton.upenn.edu
Alex Muermann	Wharton School, Univ. of Pennsylvania	muermann@wharton.upenn.edu
Michael O'Malley	Chubb	momalley@chubb.com
Phoebe Papageorgiou	U.S. Department of Treasury	phoebe.papageorgiou@do.treas.gov
Laura Petonito	U.S. Department of Homeland Security	laura.petonito@dhs.gov
Isadore Rosenthal	Wharton Risk Center	rosentha@wharton.upenn.edu
Harvey Rubin	University of Pennsylvania	rubinh@mail.med.upenn.edu
Todd Sandler	University of Southern California	tsandler@usc.edu
Peter Schmeidler	Wharton Risk Center	pschmeid@wharton.upenn.edu
Jack Seaquist	AIR Worldwide Corporation	jseaquist@air-worldwide.com
Geoff Shaw	Lockheed Martin Radiant Trust	geoff.shaw@lmco.com
Gabe Silvasi	Wharton School, Univ. of Pennsylvania	silvasig@wharton.upenn.edu
Hirokazu Tatano	Disaster Prevention Research Institute	tatano@imdr.dpri.kyoto-u.ac.jp
Craig Tillman	Renaissance Re	cwt@renre.com
Ken Travers	EQECAT, Inc.	ktravers@absconsulting.com
Jane Warsaw	Columbia University	jw277@columbia.edu
Detlof Von Winterfeldt	University of Southern California	detlof@aol.com
William Wise	ACE USA	william.wise2@ACE-INA.com
Gordon Woo	Risk Management Solutions	gordon.woo@riskinc.com
Christopher Yaure	Employers Reinsurance	Christopher.Yaure@ercgroup.com
Lester Yee	Lockheed Martin	Lester.Yee@dhs.gov