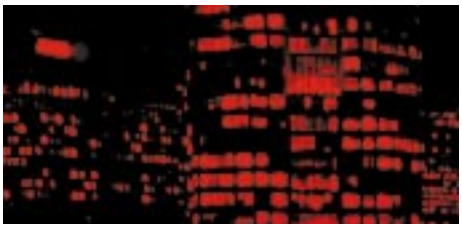
GUY CARPENTER



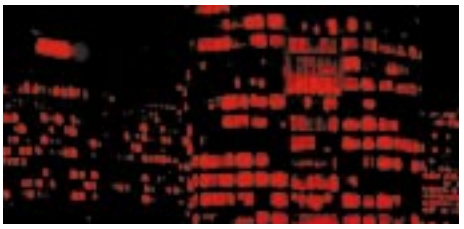
Copyright 2002
Guy Carpenter & Company, Inc.

All rights reserved.

MMC Marsh & McLennan Companies

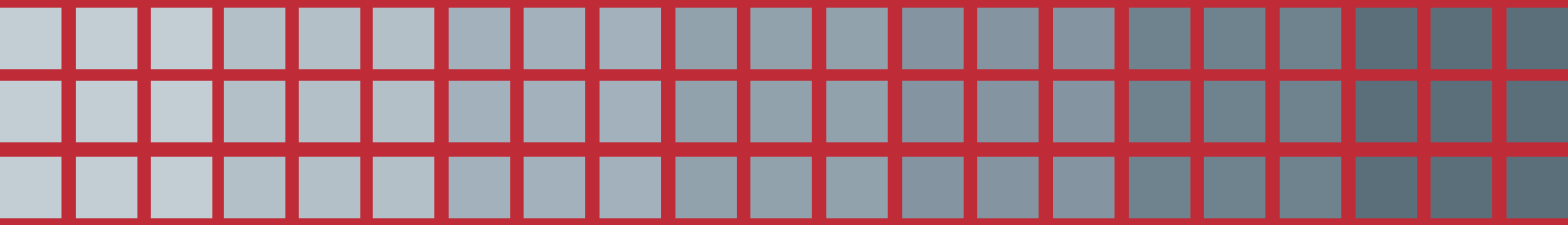
GUY CARPENTER

Seminar Report



TERRORISM

THE **TERROR** RISK: CAN IT BE MANAGED?



Questions or comments regarding this paper should be directed to:

Seán Mooney, Ph.D., Chief Economist, Guy Carpenter & Company, Inc.
212-323-1345 • sean.f.mooney@guycarp.com

For additional copies of this report, please contact your Guy Carpenter broker or contact us at **marketing@guycarp.com**

This report is also available for download at **www.guycarp.com**

Please Note:
The materials contained herein are printed with the approval of the authors. The authors' opinions are solely their own and do not necessarily reflect the opinions of Guy Carpenter & Company, Inc. The accuracy of the authors' statements is not guaranteed, and Guy Carpenter & Company, Inc. makes no representations or warranties, expressed or implied, concerning the forward-looking statements made herein. Readers are cautioned not to place undue reliance on these forward-looking statements, which pertain only as of the dates on which they are made. Guy Carpenter & Company, Inc., undertakes no obligation to publicly update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise.

Guy Carpenter & Company, Inc. provides this publication for general information purposes. It is not and should not be used as a substitute for reinsurance advice. This document is not an offer to sell, or a solicitation of an offer to buy, any financial instrument or reinsurance program.

The dissemination, use, or reproduction of this report without Guy Carpenter & Company, Inc.'s express written permission is prohibited.

Foreword

Salvatore D. Zaffino
Chairman and Chief Executive Officer, Guy Carpenter & Company, Inc.

I will always remember September 11, 2001, with deep sadness for the many colleagues and friends who were lost. Guy Carpenter's worldwide headquarters were located in the South Tower of the World Trade Center. Our sister companies in the Marsh & McLennan (MMC) family had a large number of employees in the top floors of the North Tower. Eighteen employees of our firm located in the North Tower perished in the attacks. In total, 295 employees from MMC were lost.

After the initial shock, some wondered if Guy Carpenter would survive as a firm. Our staff in New York answered with a resounding "yes," as they put Guy Carpenter's New York operations back in business in less than seven days after the attacks. We set up shop in temporary offices, re-established our technology infrastructure, and continued consulting with our clients, executing claims, and placing reinsurance, even as we all struggled with devastating personal losses.

It was not easy. But our firm moved on. I am proud to be part of such an extraordinary group of individuals.

For our industry, moving on has proven difficult, as we wrestle with losses and exposures of a magnitude previously unimagined, even by those in the business of worst-case scenarios.

Our industry, which prides itself on making sense of risk, must now develop a viable solution to events that are above all senseless. We must find an answer that does not leave insurance companies overly exposed to further catastrophic losses. We must explore the possibilities for government participation in a solution. We must discover how to measure the terror risk, price it accurately, and reach agreement on contract wording. We must meet the challenges of the terror risk head-on, much as we have addressed other seemingly insurmountable risks in history.

At Guy Carpenter, we are confident that we can do this if we work together, engage experts from within and outside of our industry, and educate each other on the realities of the terror risk.

This is why Guy Carpenter gathered the industry on March 20, 2002, not far from the scene of the worst terrorist attack in world history, for a daylong seminar exploring the question: **The Terror Risk: Can It Be Managed?** I believe that Guy Carpenter's unique experience made us a fitting host for this critical forum. It also makes it all the more appropriate that we lead our industry's response to this threat in the years to come.

While we may not be able to manage terrorism, we can surely manage the terror risk. And we will. This seminar is one step toward the solution.

Contents

Introduction

Edmund R. Megna
President, Guy Carpenter & Company, Inc.

The events of September 11, 2001, represent the largest loss in our indutry's history across numerous lines, including property, workers compensation, and life insurance. Long-term liability losses are just beginning to accumulate.

Experts agree that the terror risk is not going away. More attacks are a virtual certainty, and they are likely to be severe and unpredictable. On March 20, 2002, Guy Carpenter held a daylong seminar in New York City designed to help the industry explore ways to manage this now omnipresent risk, and continue to thrive in this new environment.

For the program, Guy Carpenter assembled an impressive group of experts from the federal government and the insurance and reinsurance industries to provide perspective on the critical issues surrounding the terror risk.

Morning sessions focused on assessing the risk and the United States government's response to the threat. Afternoon sessions spotlighted current insurance and reinsurance activities in the area of terrorism. This paper is an edited transcript of the presentations made at the seminar, and all speakers have reviewed and approved the transcriptions of their presentations.

Chapter 1, provided by Ambassador L. Paul Bremer, Chairman and CEO, Marsh Crisis Consulting, and former United States Ambassador-at-Large for Counter-Terrorism, assesses the terror risk, pointing to three trends that made the world's worst terrorist attack no surprise to those who have studied terrorism in recent years. He provides insights on the effort by the United States to combat terrorism, an effort he asserts has become the organizing principle of American foreign policy. He also discusses the lessons learned from 9/11 and the ramifications of the terror risk for business.

In Chapter 2, Paul B. Kurtz, Senior Director for National Security on the President's Critical Infrastructure Protection Board, discusses threats to America's critical infrastructure and government efforts to defend this infrastructure, including President Bush's creation of the Critical Infrastructure Protection Board. He emphasizes the urgent need for public-private collaboration in keeping America's infrastructure safe and the pivotal role the insurance industry has to play in the area of cyber security.

In Chapter 3, John S. Tritak, Director of the Critical Infrastructure Assurance Office (CIAO), and Senior Director of the President's Critical Infrastructure Protection Board, issues a strong call to action, urging an equal partnership between the public and private sectors to defend homeland security and both cyber and physical infrastructure. He spotlights areas where the contributions of the insurance and reinsurance industries can have an especially significant impact, including the modeling of terror risk and the development of a national security strategy.

Chapter 4 reflects the presentation made by Franklin W. Nutter, President, Reinsurance Association of America. Mr. Nutter explains the role the reinsurance industry has sought for government in dealing with both terrorism and natural catastrophe risk. He shares his perspective on the federal and state government response to date and outlines what he sees as the best hope for government participation in catastrophe risks going forward.

Chapter 5 features the Marsh perspective on the current terrorism insurance market, provided by Julie A. Martin, Vice President, Marsh. This comprehensive overview explores the various terrorism exclusions on property cover, factors affecting premiums, current markets for stand-alone terrorism cover, and what the future holds for property terrorism risks.

In Chapter 6, Mary N. Guzman, Senior Vice President, Marsh, discusses the dangerous misconceptions that exist about "e-risk," the major categories of cyber risk, and the reasons why "traditional" policies do not respond to the cyber world. She also forecasts significant changes in the market for cyber-risk insurance. These changes will come as companies accept that no "silver bullet" technology holds the answer, and that insurance, along with heightened cyber-security standards and practices, will provide the solution.

Chapter 7 presents a panel discussion on insurance and reinsurance for cyber risks, moderated by Harrison D. Oellrich, Managing Director, Guy Carpenter. Presentations are provided by four experts on the topic: Jeffrey S. Grange, Vice President and Global Manager, Financial Fidelity Products, Chubb Group of Insurance Companies Department of Financial Institutions; Ty R. Sagalow, Executive Vice President and Chief Underwriting Officer of AIG e-Business Risk Solutions℠; Sandy G. Hauserman, Senior Vice President, Guy Carpenter; and Lee M. Zeichner, President, LegalNet Works, Incorporated, a company that advises public and private organizations on legal and policy issues relating to critical infrastructure laws and regulations.

In Chapter 8, Seán Mooney, Chief Economist of Guy Carpenter, moderates a question-and-answer discussion on reinsurance and terrorism with a panel of Guy Carpenter colleagues. The discussion spans a range of topics, including the status of terror reinsurance cover at January 1, 2002, renewals; the development of tools for modeling terror risk; stand-alone terrorism coverage; and critical contract wording issues.

Rounding out the program in Chapter 9 are presentations by Britt Newhouse, Managing Director, Guy Carpenter, and Christopher B. Royse, Principal, Guy Carpenter, discussing reinsurance solutions for terror issues. Mr. Newhouse offers an optimistic viewpoint, comparing the terror risk to another exposure the industry once considered "unmeasurable and unmanageable"—that is, the risks relating to the riots and civil unrest of the 1960s, which were ultimately addressed by the industry. Given the industry solutions already evolving, the terror risk may be no different, according to Mr. Newhouse. Mr. Royse outlines a solution already in development to enable regional carriers to manage the terror risk. The concept, a regional insurer pool, has already been received with enthusiasm by reinsurers.

Finally, this paper also includes a brief summary of "Next Steps" for addressing the terror risk by the moderator of the seminar, Gregory T. Doyle, Executive Vice President, Guy Carpenter. The steps outlined, Mr. Doyle emphasizes, must be taken by the public and private sectors together.

Guy Carpenter is grateful for the contributions of all program participants, both in preparing and presenting their materials at the meeting, and for their assistance in compiling this report. Their expertise and insights bring our industry closer to addressing the many complex issues involved in managing the terror risk.

CHAPTER 1

Assessing the Terrorism Risk

Ambassador L. Paul Bremer
Chairman and CEO, Marsh Crisis Consulting, and former United States Ambassador-at-Large for Counter-Terrorism

The attack of September 11 was the world's worst terrorist attack to date. But it also represented much more than that. It crystallized the nature of the threat to American national security in the 21st century—a threat that has broad implications for American security, for international relations, and for business, both in the United States and abroad.

THE THREAT

September 11 outraged all of us, but it did not surprise those of us who have studied terrorism over the past few decades. The attacks are not surprising in that they reflect three underlying trends, namely:

- A shift in the nature of terrorism
- Changes in the geo-political situation
- Tensions between Islam and the West.

The Shift in Terrorism

There has been a dramatic shift in the kind of terrorism the world has faced since the late 1980s through the 1990s. Terrorism in the 1970s and 1980s was used as a tactic to draw attention to a cause. Terrorists would carry out a shocking event, draw media attention, and then explain their cause in the hopes of finding resonance in the public at large. Their motives were relatively modest.

These terrorists had a form of self-restraint in terms of the outrages they would commit. Their intention was not to kill a lot of people, but rather to generate a lot of attention.

Beginning in the late 1980s and throughout the 1990s we saw a dramatic shift in the motivation of the most important terrorist groups. The new terrorists are motivated by hatred, revenge, and religious extremism, such as we have seen in Al Qaeda. Some are driven by apocalyptic visions of the world, like the Aum Shinrikyo group that attacked the Tokyo subway system in 1995.

Illustrating this shift is the fact that there were fewer terrorist incidents in the 1990s, but the number of people killed as a result of terrorist incidents rose. Unclaimed or anonymous attacks also increased dramatically during

Those who hate us cannot attack us with conventional means.

the 1990s. In contrast, old-style terrorists took responsibility for events and created the opportunity to bring their cause to light.

Today's terrorists are also willing to give their lives for terrorism. In 1988, the CIA reported that less than 2 percent of all attacks from 1968 to 1988 involved suicides. During the 1990s, there was a dramatic shift to suicide terrorism, virtually eliminating traditional deterrent strategies such as jail time. Suicide terrorists are not despondent and downtrodden. Like the terrorists of 9/11, they die out of hope, not out of despair.

These changes in terrorist motives create very different problems.

The Geo-Political Environment

The second global trend relating to the attacks of 9/11 is the unique geo-political situation in which the United States finds itself in since the collapse of Soviet Communism.

The United States is now the world's only superpower. We are in a position of political, economic, military, and cultural domination that is without precedent in recorded history. There is no previous example of a nation being as dominant relative to the rest of the world as the United States is today.

While domination creates opportunities, particularly for business and for diplomacy, it also creates resentments. Those resentments are particularly strong in many poor parts of the world.

This geo-political situation was evident during the Gulf War a decade ago. When the United States attacked Saddam Hussein in January of 1991, Hussein had the fourth largest army in the world, well equipped with modern Soviet weapons, both ground and air. The United States swept it aside in a matter of days.

The lesson was clear: those who hate us cannot attack us with conventional means. Those nations that hate America will have to resort to what the Pentagon calls "asymmetric" or unconventional warfare. Terrorism is the ultimate unconventional warfare.

Islam vs. the West

The third trend is the growing tension between Islam and the West. Resentment against America's domination is particularly strong in parts of the Muslim world. This relates in some ways to Islamic history over the last 300 years. There is a sense among many Islamic thinkers that Islam has been in a state of decline ever since the defeat of Islamic armies at the gates of Vienna in 1683. This is historically correct: there has been a massive economic and political failure in much of the Islamic world during their post-colonial era.

Today, the Middle East has 17 percent of the world's population and

just 3 percent of its trade, excluding oil. In the year 2000, approximately 300 books were published in all of Egypt. That is less than the number published by the average university press in the United States.

What went wrong? During the 250 years when much of the Islamic Middle East was under colonial authority, French and British, Muslims could blame the colonial authorities for their problems. They could play them off against each other.

As the colonial period was ending in much of the Islamic world, the Cold War began. Instead of playing colonial masters against each other, the same countries could now play the United States against Russia.

Such maneuvering distracted the attention of many of these countries' leaders away from the need to modernize economies and political systems. As a result, the political systems in much of the Islamic world today are very brittle. And there is economic failure, even in countries with abundant oil.

It is correct to state, as President Bush has, that we are not at war with Islam. There is, however, a civil war raging within Islam. We have seen it fought over the last six months. It is a civil war between moderate Islamic leaders, who believe that Islam can peacefully coexist with the West, and groups such as Al Qaeda, which tries to define Islam as a radical religion that cannot live in peace with the West. The United States and its allies have a huge stake in the moderates winning this civil war.

For the next decade, at least, the United States will not face anti-hegemonic forces. No one country or group of countries is likely to rise to challenge America in that period. But while the United States may not need to worry about a new superpower rising up in the near future, we do need to be concerned about another challenge, one much like that we confronted between the 17th and the 19th centuries: the challenge of bandits, warlords, pirates—and now terrorists. These are amorphous enemies, hard to grasp and difficult to defeat.

These groups and states that hate us know they cannot defeat the West conventionally. This raises the specter of weapons of mass destruction—including chemical, biological, nuclear, and radiological weapons.

Over the past decade an enormous amount of information about these weapons—information that was previously restricted to specialists—has become widely available through the Internet. Today the Internet is a source of recipes for growing anthrax or for building radiological dispersal devices, or "dirty" bombs.

The United States Department of Energy's Web site, for example, includes the locations of all of America's nuclear power plants and nuclear waste facilities.

Technology has made available information regarding biological agents, which can be astonishingly lethal. Properly dispersed, one tablespoon of anthrax has the capacity to kill 250 million people.

There is concern about smallpox. A World Health Organization study concluded that smallpox killed between 300 and 500 million people

September 11 was not just a terrorist attack; it was the face of the new threat.

during the 20th century, more than the number killed in all of the century's wars combined. There is concern that the recent sequencing of the human genome will spur the design of new viruses, against which there are no vaccines or antitoxins.

Clearly, technology is a double-edged sword. It greatly accelerates the pace of progress but it also allows what some scholars call the "privatization of violence." Individuals now have the power to challenge every government's most basic responsibility—the security of its citizens.

THE RESPONSE

What is the response to this threat? The administration has recognized that this marks a turning point in American national security policy. September 11 was not just a terrorist attack; it was the face of the new threat.

Combating the threat has become the organizing principle of American foreign policy. In order to counter the threat, we must deny terrorists territory. Groups like Al Qaeda cannot be allowed to operate in a welcoming environment like Afghanistan. That has to be changed.

Three Phases

Accordingly, phase one of the counter-terrorist struggle was conducted with the dual objective of eliminating the Taliban and destroying as much of Al Qaeda's Afghan infrastructure as possible.

Phase two of the operation, currently underway, aims to break up Al Qaeda cells in several dozen countries around the world. CIA Director Tenet testified that more than 1,000 terrorists have been arrested in many countries around the world. Many of these are "sleepers," who infiltrate society and are difficult to root out. Rooting them out requires an enormous amount of cooperation between intelligence and law enforcement agencies. That cooperation is happening.

The third phase is to address what President Bush termed the "axis of evil," citing Iran, Iraq, and North Korea. This includes terrorist groups, states that support terrorism, and states with access to weapons of mass destruction.

Five of the seven states known to support terrorism have nuclear, biological, and chemical programs. Iran, Iraq, and North Korea are among those five, so it is correct to identify them as an important "nexus" for United States attention in phase three.

A Change in Strategy

The President has signaled a shift in America's strategic posture towards terrorism. During the 1990s the United States government waited until terrorists attacked, then responded. This strategy is not sufficient when weapons of mass destruction are part of the equation.

Over the last 30 years, 80 percent of terrorist attacks against American interests have been against American businesses.

The administration is transitioning from a wait-and-respond policy to a detect-and-prevent strategy. This is a much more forward-leaning, preemptive, and preventive approach to terrorism, and relies on more and better intelligence.

LESSONS LEARNED

A number of lessons are emerging from 9/11. First, the events of that day debunked the myth of triumphant idealism, which implies that there is no real alternative to Western liberal democracy and open markets. September 11 brought us back to the reality of power and how the world works.

September 11 ended the myth of American invulnerability. We were attacked by a hostile force on our own continental shores for the first time since 1812. The event renewed the critical need for military force, which had been challenged since the end of the Cold War.

The most important lesson from 9/11 is that there is no substitute for American leadership. With global domination comes an immense responsibility for world stability and security. Nobody else can do it. The 9/11 attack could have taken place in Berlin, Paris, Rome, or London. If it had, not one of those countries could have responded as America did. They simply would not have had the capability.

Moreover, these countries could not have responded in a unified fashion—a fact that has spurred Europeans to think deeply about whether they have the capacity to mount their own military and security policy.

The final lesson of 9/11 relates to America's new thinking about security. The government must reassess how it is organized to handle security. The creation of the Office of Homeland Security is a start. Much more remains to be done.

RAMIFICATIONS FOR BUSINESS

Over the last 30 years, 80 percent of terrorist attacks against American interests have been against American businesses, and United States corporations will continue to be a target of terrorist attacks. It is expected that Al Qaeda, either as an organized group or with relatively autonomous units presumably still available in the United States, will strike again. As a result, businesses are forced to operate in an environment of heightened risk and uncertainty.

Political Risks

The political risks of doing business in emerging markets have increased and will continue to do so. Some of this rise is related to terrorism and the war currently underway, which heighten political risk in places like the Middle East, Pakistan, Indonesia, and Malaysia. Yet even before 9/11 the risks of doing business in emerging markets was on the upswing—due to

Indeed, there are going to be uncomfortable moments for all of us.... Hopefully there will be more uncomfortable moments for our enemies.

globalization, or more specifically, due to the disparate impact of globalization.

Globalization—the free movement of goods, people, ideas, and data across borders—has immediate, negative impacts on emerging market countries and societies before it has positive effects. A recent United Nations study looked back over the 1990s and detailed the number of countries and people left behind in that decade of globalization. The study revealed that per capita income in countries with a total population of 2 billion—about one third of the people in the world—declined an average of 1 percent a year during the 1990s.

This is a good example on a macro scale of the disparate impact of globalization—a fact that fuels political instability as well as the classic problems for which one purchases political risk insurance, such as nationalization and currency inconvertibility.

Unexpected Crises

September 11 taught business to expect the unexpected. Large American companies will face a crisis every four to five years. This means that every CEO and every senior executive will have to manage a crisis during his or her tenure. Crisis management planning is vital: there is no substitute for preparing for a crisis before it hits.

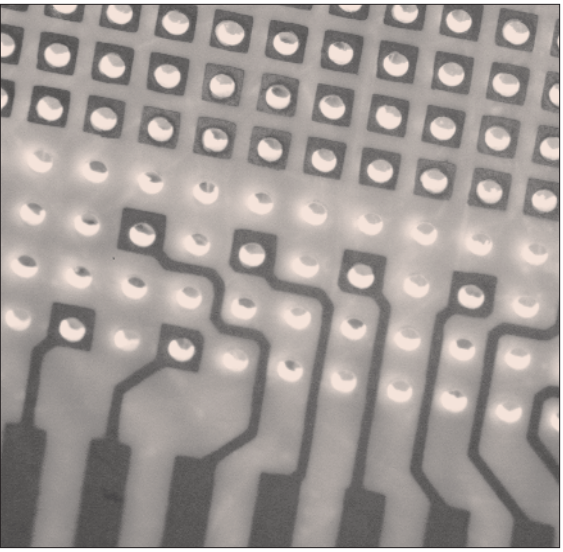
September 11 also showed the new face of the threat to American security in the 21st century. Deep underlying trends suggest that we will continue to face this threat in the years ahead. As was the case during the last half century, American leadership is going to be vital to overcome this threat. This is going to be uncomfortable at times for Americans and particularly for American diplomats, because people resent a great power exercising leadership. But there is no alternative.

Indeed, there are going to be uncomfortable moments for all of us, because terrorism is not going to go away. Hopefully there will be more uncomfortable moments for our enemies.

CHAPTER 2

Cyber Threat and Response: A Macro View

Paul B. Kurtz
Senior Director for National Security,
The President's Critical Infrastructure Protection Board



September 11 taught us many things. Before 9/11, many thought that Al Qaeda and Osama bin Laden were overseas nuisances, responsible for the tragic bombing of the United States embassies in East Africa and the attack on the USS Cole. The threat was over there; even though Osama bin Laden was behind the 1993 attack on the World Trade Center.

As a result of 9/11, we learned that our enemies are capable of conducting sophisticated attacks, taking advantage of our free and open society. We also learned that infrastructure is a target: the destruction of 16 acres of property in lower Manhattan dramatically illustrates that point.

In addition, we learned that we cannot plan for the future based on past attacks. We could not have prepared for the attacks on the World Trade Center based on the attacks against the embassies in East Africa. Similarly, we cannot use the World Trade Center attack as the sole basis for future planning. Something different could happen next time, including an attack on our information infrastructure.

Finally, we learned that the worst case scenario can happen. What if the extreme physical attack of 9/11—that catastrophic assault on our infrastructure—were combined with an attack against our information infrastructure? These are the "what ifs" we must now consider.

Possible actions against our information infrastructure include disruption of key networks that support critical infrastructure—such as oil and gas, power, water, or emergency services. In addition to the destruction of networks and data, such actions might entail the corruption or distortion of data. Any one of these actions could have cascading effects throughout multiple sectors and industries.

THE CRITICAL INFRASTRUCTURE PROTECTION BOARD

Shortly after taking office, President Bush convened his cabinet to discuss information infrastructure security. Many cabinet leaders came from the private sector, and they quickly recognized that the federal government is quite antiquated with respect to the security of its information infrastructure. The President realizes that the IT revolution has affected the way

business is conducted, the way our government operates, and the way we mount our national defense.

Following 9/11, the President signed an executive order that reorganizes the way the government views the issue of infrastructure security. The presidential policy states that it is the charge of the United States government to protect our information infrastructures in order to help protect our people, our economy, our essential human and government services, and our national security. Such protection also means making sure that any disruptions that do occur are infrequent, minimal in duration, and manageable.

President Bush created the Critical Infrastructure Protection Board to coordinate the protection of our information infrastructures and the physical assets that support them. The board's chairman, Dick Clark, serves as special advisor to the President for cyberspace security, and reports to the national security advisor and the chief of homeland security. The board has senior-level representation from most of the federal agencies in Washington and coordinates broad policy on the issue of information infrastructure protection.

Creation of this board recognizes the new world in which we live. We are an interdependent society, deeply reliant on information technology. All of our major industry sectors—manufacturing, oil and gas, power, transportation, healthcare, telecommunications, information technology, banking and finance—are interrelated. An attack on any one sector can directly impact others.

Board Responsibilities

The Critical Infrastructure Protection Board has numerous responsibilities, each of which is addressed by a standing committee. These responsibilities include:

- Security of government information systems
- Outreach to the private sector
- Incident coordination and crisis response
- Addressing the global deficit in IT security personnel
- Recruitment and training programs
- Research and development issues
- Law enforcement coordination
- Global outreach and coordination

Five Truths About Information Infrastructure

Effectively protecting our information systems begins with understanding five truths about information infrastructure.

1. Current information networks were not designed with security in mind. The Internet was first developed in the late 1960s and early 1970s as a means of exchanging research data among universities. It was not originally envisioned as the critical element of our information infrastructure that it has become.
2. Networks will never be completely secure.
3. There is no single "silver bullet" solution for information infrastructure security, and the problem must be addressed by technology, policies, and people working together.
4. No single government agency can handle the problem of infor-

Viable solutions will only come out of a partnership between government and the private sector.

mation infrastructure security. Everybody has a role to play.

5 Viable solutions will only come out of a partnership between government and the private sector. After all, the private sector owns and operates 85 percent to 95 percent of the critical information infrastructure.

THE ENEMIES OF INFORMATION INFRASTRUCTURE

The enemies of our information infrastructure include:

- "Scriptkiddies"—a term I use to refer to an attacker who possesses no expert knowledge and no real capability, but simply acquires malicious software through the Web.
- Criminal organizations
- Terrorist organizations
- States or companies engaged in espionage
- Nation states

Finding the Enemy

Finding the enemy is difficult, costly, and time consuming, for many reasons. First, an attack against critical information infrastructure can be launched from virtually anyplace on the planet. It could be launched by a foreign party in the United States against the United States, or initiated from Germany and executed by an Iraqi. "Spoofed" attacks—in which you do not necessarily know where the attack was initiated—further complicate the problem.

The challenge is also compounded by the frequent involvement of insiders. Most victims look outside their own organizations first. Corporations and the government have to understand that an attack may come from within or with inside assistance.

Yet another complication in finding the enemy is the fact that deliberately tainted or "sleeper" software may be in play. This is software that has been deliberately tampered with, without the buyer's knowledge, prior to purchase.

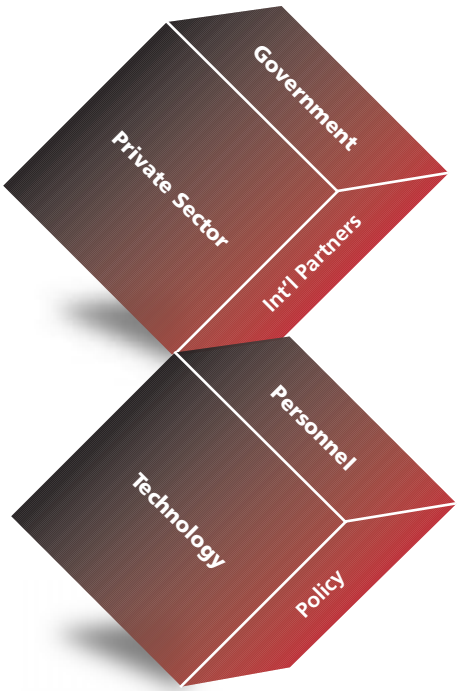
THE DEFENDERS OF INFORMATION INFRASTRUCTURE

There are many potential defenders against information infrastructure attacks. These include the owners and operators of infrastructure; key private sector IT vendors; federal, state, and local governments; the military; and nonprofit organizations, such as CERT, the Center for Internet Security Expertise at Carnegie-Mellon University.

Global partners are also critical defenders. Many of these threats emanate from places with which the United States does not have close relations at the present time. We need to develop and foster relationships with allies overseas to work on this problem.

CYBER SOLUTION CUBE

The Six-Sided Solution



Source: Paul B. Kurtz

THE NEW REALITY

The new reality is that no single entity can provide defense on its own. We need to work together. Cold War methods will not provide early warning or defense in this new world. A radar in Alaska seeking missiles coming over the top of the pole is not going to be effective. Every critical sector of the economy needs to act as a radar, always watching for the next attack. Moreover, an attack against our government might not target the government directly. It could aim at banking and finance, oil and gas, or another sector in an effort to disable the economy.

Given this new reality, nothing is more crucial for combating information infrastructure attacks than a public-private sector partnership. It is the only way we are going to find viable solutions.

Fortunately, private sector perceptions regarding security are changing, as illustrated by recent comments from the top executives at Cisco, Microsoft, and Oracle. Cisco President and CEO John Chambers recently announced that security and reliability must now be job one for his company. He has good business reasons for bringing security and reliability to the forefront, and he notes that Cisco cannot do it alone. He has pledged to work with others in this effort. In addition, Bill Gates is working to see what Microsoft can do to bring greater security and reliability to its products, and Larry Ellison of Oracle has shown a willingness to change perceptions and work with others on this issue.

NATIONAL STRATEGY

The Critical Infrastructure Protection Board is charged with developing a national strategy with the private sector. There are a number of audiences for this strategy. They include home computer users, small businesses, and operations at the enterprise, sector, national, and international levels—for which broad issues such as domain name servers and border gateway protocol issues need to be addressed. Most of the strategy is being developed by the private sector. The strategy must be dynamic—not simply a coffee table book or a large, hard-to-read manual that sits on a desk.

Key questions to be addressed in developing this national strategy for information infrastructure security include the following:

- Have critical information systems and interdependencies been identified?
- Are the vulnerabilities of these dependencies understood?
- Are the right programs, policies, technologies, and organizations in place?
- Are recovery and reconstitution programs in place?
- Are the risks understood?

The Cyber Solution

The process of developing a national solution for information infrastructure security can be conceptualized as a six-sided cube, with each side representing a vital partner or component in the development of the solution. These six components include the private sector, government, international partners, personnel, technology, and policy.

If any one of these components is left out, a side of the cube is missing—and we have left ourselves open to risk.

CHALLENGES

Several challenges lie ahead for all of those involved with this issue. These include:

- Increasing awareness and improving risk management.
- Making cyberspace more secure as the IT revolution continues to unfold—a task that is much like trying to paint a speeding train.
- Implementing security solutions in partnership—with the public and private sector working together.
- Creating an environment that fosters the sharing of information, so that problems with a particular system or network can be addressed without revealing proprietary information that could be used by a competitor.
- Developing common metrics for understanding the information infrastructure security problem, and modeling the interdependencies that exist within our infrastructure among various economic sectors. By so doing, we can understand how an attack in one sector affects players in other sectors.
- Addressing the shortage of qualified IT security personnel.

ROLE OF THE INSURANCE INDUSTRY

The insurance industry has a pivotal role to play, particularly by developing cyber insurance policies. This may be easier said than done due to the current lack of information. But carriers must begin to develop the means with which to write such policies.

Perhaps cyber-risk policies can be written mandating that insured parties employ rigorous cyber-security measures, or they may be written with coverage exclusions for "acts of war."

Somehow it can be done. We at the federal government want to know how we can help make it happen, and we encourage a continuing dialogue on this critical topic.

CHAPTER 3

Public Sector Perspective on Risks Associated with Terrorism: Concern and Collaboration

John S.Tritak
Director, Critical Infrastructure Assurance Office (CIAO) and
Senior Director, President's Critical Infrastructure Protection Board

Photo source: unknown

While what happened on 9/11 was a shock, sadly it was not a surprise. Guy Carpenter, Marsh, AIG, and many others in the insurance and reinsurance industries had been worrying about the threats to critical infrastructure for a while. Today, homeland security and critical infrastructure protection have become timely phrases, but they were on the lips of many in insurance and reinsurance even before 9/11, albeit in a different context.

Critical infrastructure assurance has been in play for some time. Had it not been, the situation would have been far worse after 9/11. As it was, half of Wall Street had to relocate, yet the stock exchange was up and running on the Monday following the Tuesday attack. This is a testament to sound risk management in practice and to the emergency preparedness brilliantly demonstrated by the financial services industry and others.

DON'T WAIT FOR GOVERNMENT ACTION

The industry was on the right track with its concern over critical infrastructure protection. Because when it comes to critical infrastructure protection, the private sector must not wait for the government to tell it what to do. Business cannot wait for government to solve this problem behind the closed doors of the Oval Office or in the inner sanctums of the Pentagon or State Department. This is a national security problem the government cannot solve alone. Private enterprise must be actively involved in developing a solution.

Osama bin Laden has declared that the target is the United States economy —and that puts the private sector on the frontline. More and more, terrorism is going to focus not on political targets and military installations, but on the private sector. Increasingly, we rely on an interconnected, interdependent global digital nervous system to operate our physical, industrial assets.

Because of this interdependence, it is possible to create disruptions not just within any particular economic sector, but across numerous sectors. Terrorists will seek to exploit this vulnerability.

When United States troops stormed abandoned Al Qaeda facilities they discovered plans to disrupt water facilities, the financial services industry,

When it comes to critical infrastructure protection, the private sector must not wait for the government to tell it what to do.

and other sectors. Many of these plans included disruption of the information systems and networks upon which industries operate.

How effective such an attack might be is uncertain. But we know that it is being considered, and IT security experts will tell you that there are many ways to infiltrate information systems and networks.

Provide Incentives for Risk Management

When I first became Director of the Critical Infrastructure Assurance Office after leaving the private sector three years ago, the basic policy was that since the private sector owns and operates the vast majority of the national infrastructure, the private sector should do more to protect critical infrastructure. The government should step in only where the private market fails, and should explore options to bridge any gap between business motivations and national homeland security interests.

I was also told that a real hope for the future, in order to spur businesses to invest in higher levels of information security, was to get insurers to underwrite insurance that would provide incentives to pursue this greater level of investment. Some insurers are doing this. But as profit-driven businesses, there is a limit to how far insurers are prepared to go with coverage.

So the question is, how can we provide an incentive for companies to invest in information security? The risks of America's dependence on information systems and networks, particularly the risks associated with interdependency, are beyond our ability to define in scope. While insurers may be able to underwrite exposures at the lower end of the risk spectrum, the higher end remains a challenge. Can that challenge be met? I am not in the position to say today, but I can suggest some ways we can move forward.

Shift the Current Mindset

First, there must be a fundamental shift in the way we think about the role of government as opposed to the role of private industry.

In the past, national security was something the private sector essentially outsourced to the government and paid for with taxes. But the definition of national security has changed and broadened as a result of 9/11. Now the government is charged with protecting the American way of life at home, projecting power overseas, and maintaining our country's global alliances. We have a military second to none, but we need more.

Our enemies mean to undermine America's way of life, either directly or indirectly, by corroding public confidence in our public institutions, and to secure against this we must have a public dialogue, shaped by both public and private sector voices.

Create an Equal Partnership

Government and industry must come together as equal partners

Clearly, the responsibility for protecting our critical infrastructure must be shared by government and the private sector.

and develop common approaches to protect their mutual interests.

There is some question about the extent to which government will be involved in physically protecting the economic assets of the United States. Prior to 9/11, the government did this indirectly. Government protected our air space and our borders. The FBI apprehended potential criminals and terrorists, and as a result protected our infrastructure. Now we face a different challenge.

Companies also have new concerns and responsibilities. CEOs have renewed concern over the physical protection of company property and assets. Businesses are taking a hard look at what more can be done to safeguard physical facilities against attack. However, there is a limit to how much industry can do on its own to protect against physical attacks. There was nothing, for example, that the World Trade Center could have done to prevent someone from turning a 767 into a cruise missile.

Clearly, the responsibility for protecting our critical infrastructure must be shared by government and the private sector.

Reassess the Cyber Threat

Many companies wonder what the likelihood is of their coming under terrorist attack. In reality, the chances of falling victim to an attack like that on the World Trade Center are low. But the chance of someone exploiting vulnerabilities in a company's network or IT systems is much higher, and companies must find ways to manage that higher risk.

When people talk about "cyber risk," they typically use the term to the exclusion of physical threats. This has a distorting effect on the risk assessment. The cyber and the physical are inextricably linked in many cases.

In assessing cyber risk, a company should start by considering what it delivers. Where does its revenue stream come from? What are the vital services it provides to the market, which, if disrupted for periods of time, could have a significant impact on customers or investors? Working backwards from there, a company can assess its value chain and ascertain its vulnerabilities.

These vulnerabilities may arise from physical assets, from human beings, or from information systems and networks. To the extent that an information system and network is part of the value chain, a company must make choices about the various tools available to mitigate the risk, and consult experts to evaluate the probability of system and network exploitation.

If every company undertook such a process of information assurance, great strides would be made in defeating those who want to disrupt our economy.

There are also initiatives an individual enterprise can undertake

Soon information assurance—read business continuity, read business assurance—will be as important to the CEO as marketing and product development.

to help secure the system within which it operates. But these only make sense if everyone else in that system is doing it too. So how do you create a mechanism that takes us closer to a market-based risk management solution?

Modeling the interdependencies of the economy and the major stakeholders in that economy is an important first step. It is also an area in which it is acknowledged that government investment is required.

Efforts are underway within the federal government to map and model the interdependencies and consequences of disruption across various economic enterprises. But these models will be only as good as the input provided by the private sector. The electric power industry, the banking and financial services industry, and the insurance industry can all provide important input to this process and can also become major consumers of the product.

OPPORTUNITIES FOR PUBLIC-PRIVATE PARTNERSHIP

Every time I talk with insurers about cyber risk, I am told that there are no actuarial data, and that without data, insurers cannot define and bind the risk.

This is one example of an area in which government and industry can work together. Effective modeling can help simulate or at least partly define and quantify the cyber risks confronting enterprises today. Such modeling can, in turn, help shape the way the reinsurance market addresses these problems.

Another important area in which industry and government can work together is in defining elements in the statutory or regulatory environment that should be eliminated. I am sure every company would like to provide a tsunami of recommendations, so let me suggest a refined approach.

There are a number of reporting requirements by which many regulated industries must abide. Until very recently, for example, the electric power industry was required to essentially map online —in real time—the purchase and sale of electric power across the country. If I were buying a quantity of electric power from Virginia, say, I would put in a bid and a probabilistic model would determine whether or not transmission and generation capacity would be available to meet my load requirements.

If a blue line appeared, it would mean yes, requirements could be met. A red line would mean no. The implications of a red line would catch my attention. Many of these red lines appear from time to time, and by tracking them one could map the stresses and strains of the electric power grid.

The insurance and reinsurance industries have much to bring to the table in this endeavor. They can help the United States government better understand the challenges.

One could also potentially exploit the fact that certain parts of the electric power grid are being stressed to their fullest capacity, so disruptions to these parts of the grid could have a disproportionate and perhaps cascading effect on the economy as a whole.

So why is this publicly accessible mapping done? Because transparency in the purchase and sale of electric power is a public good. In America, we do not want any particular group cornering the market.

In this case, two different public interests—security and transparency—may be in conflict. The best solution is one that would satisfy both interests. Finding that solution requires action by both government and enterprise. Enterprise knows where the problems lie better than government. Private sector businesses are far better positioned to point out a particular law or regulation that may be inconsistent or obsolete in these changed times. Tell government where these problems lie and government has an obligation to consider them.

Over time I would like to see a statutory body that induces and rewards such proactive behavior and is conducive to voluntary action.

A NATIONAL STRATEGY

In many respects, the value of a national security strategy is not in the end-product alone, but in the process of getting there. We need to create a consensus between the public and private sectors as to the security concerns and the responsibilities—and lay a path to a common, agreed-upon outcome.

The insurance and reinsurance industries have much to bring to the table in this endeavor. They can help the government better understand the challenges.

There should also be an educational component to this strategy, one that will create a better understanding of the issues that will lead government and industry to a mutual solution.

So I urge once again, do not simply wait for the government line. On Capitol Hill, there is an underlying sense that industry is not going to get this right. Profit motive will stand in the way, and industry will not act in the national interest, or at least not in the national security interest.

I have seen enough of what has been happening in the private sector since 9/11 to know that this is absolutely not true.

If government feels nothing is being done by the private sector to address these problems, then it has an obligation to act. You can help the government get this right. The government will do its part as well.

CHAPTER 4

The Federal Solution: Where Are We Today?

Franklin W. Nutter
President, Reinsurance Association of America

The following comments consider the role the insurance industry has sought from the government in dealing with both terrorism and natural catastrophe risk, and the role that the state and federal governments believe they should play.

CURRENT APPROACHES AT THE STATE LEVEL

Rate and form regulations mandated by the states are clearly a problem for the industry in addressing catastrophic risk. The fundamental ways that state governments finance catastrophic exposure—mandatory coverages, limits on exclusions, including risk of terrorism, and prior rate approval—inhibit the process of managing and financing catastrophic risk.

There is an unfortunate reluctance on the part of the states to accept catastrophe modeling in the regulatory process. While catastrophe modeling is consulted, state regulators resist using it as a basis for rates and exposure analysis.

With respect to catastrophic risk, the philosophy of the states has been to appropriate the private sector—specifically, by using residual markets, catastrophe pools, and Joint Underwriting Associations (JUAs)—without allowing the industry the underwriting prerogatives normally associated with the private market.

There are currently three well-known state-based public and private sector partnerships for catastrophic risk:

- The California Earthquake Authority involves a compromise by the industry to strike a middle ground between being required to offer homeowners coverage for earthquakes in California versus being required to capitalize a private-public partnership to provide consumer coverage.
- The Florida Hurricane Fund is an example of a public reinsurance mechanism financed by public and private sources. In each of the last legislative sessions, the insurance commissioner in Florida has sought to expand the role of this government-sponsored, quasi-private-public partnership to squeeze out private sector opportunities to write catastrophe hurricane risk in that state.

- The Hawaii Hurricane Fund is no longer active, but a proposal is pending in the Hawaii legislature to take money collected in the fund, redirect it to the state's fund for workers compensation, and create what is essentially a private insurance company funded by public money. This is also in competition with the private sector.

CURRENT APPROACHES AT THE FEDERAL LEVEL

Existing federal approaches to financing catastrophic risk include the traditional FEMA response and recovery in the immediate aftermath of an event. Other federal agencies also finance the immediate response to catastrophes.

One element of federal law that provides for financing catastrophe risk is the tax system, in that it gives insurance companies the authority to carry back or carry forward losses associated with natural catastrophes and catastrophes associated with acts of terrorism.

Other federal programs include:

- The National Flood Insurance Program, under which the insurance industry provides an administrative mechanism, but the government bears the risk of residential and small commercial flood loss.
- The Price Anderson Act, which provides the framework for third-party liability associated with nuclear plants. It is a public-private partnership that involves private money pooling mechanisms to create a means by which to finance liability associated with nuclear accidents.
- The National Insurance Development Program, which no longer exists, was a federal program developed after the riots of the late 1960s to provide reinsurance for riot-related loss. In exchange for this program's formation, the industry had to support the creation of Fair Access to Insurance Requirements (FAIR) plans to provide property coverage in the states.

The riot reinsurance program and other current programs exemplify some of the ways in which the private and public sector can work together at the federal level to address catastrophe risk.

A RETROSPECTIVE

A retrospective of federal initiatives rounds out the perspective on how, over the last decade, the insurance industry has aggressively sought to create a role for the federal government and the private sector in financing catastrophe exposure.

The first such initiative was a proposed federal loan plan, a mechanism that provides loans to private sector insurance companies to address liquidity issues associated with huge natural catastrophe losses.

This early effort was not well received by the industry, largely due to concerns that it is not financially responsible for a company to add debt at the same time that it pays enormous losses. Rating agencies and analysts would probably not view this as an attractive proposal either.

A second proposal called for an all-risk insurance policy to spread the

The House of Representatives has passed legislation providing a role for the federal government in reinsuring acts of terrorism.

risk of catastrophes, including various types of natural catastrophes, across the country's entire policyholder base. While this concept is attractive to agents marketing coverages to consumers, and perhaps also to brokers marketing to commercial consumers, insurance companies did not want the "take all comers" type of approach it implies. They want to underwrite; they want to select and price risk.

Over the last few years the industry has engaged most aggressively in a variety of initiatives promoting government-sponsored enterprises, effectively creating government pools. Examples of such government-supported entities in other sectors include Fannie Mae, Freddie Mac, and the United States Postal Service, which are government-sponsored enterprises that operate like private businesses, but with some government guarantee or government backing, at least at the start.

This concept has been viewed by the insurance industry as providing liquidity and some potential tax preferences, while at the same time offering some financial protection for the industry and for consumers.

In the mid-1990s the industry sought to promote a government-sponsored enterprise that would provide consumer coverages for natural catastrophes. This is analogous to the flood program, but with a private sector role in running and perhaps financing the program.

There were also reinsurance approaches based on government-sponsored enterprises. The first was a quota share approach, with the government establishing a program but having a risk-sharing arrangement with private sector companies participating in the program. Another was a program that would effectively provide excess-of-loss coverage for the industry.

Yet another approach involving government-sponsored enterprise called for reinsuring state catastrophe funds—the California Earthquake Authority, the Hawaii Hurricane Fund, and the Florida Hurricane Fund. This idea was not embraced, since the industry did not want to encourage the creation of other state funds in an area where it was seeking to provide coverages.

The tension is evident: the private sector wants to preserve market opportunities, yet is not comfortable assuming the entire exposure.

The idea that gained the most traction in the last session of Congress was a proposal to auction federal catastrophe capacity. The Treasury Department would auction excess-of-loss contracts, providing capacity over and above the private sector's capacity. As proposed, these catastrophe contracts could be divisible. An organization like

Guy Carpenter could purchase the contracts and sell them, or use them to provide capacity among its client base. Contracts could be regional, since certain regions of the United States are more prone than others to extraordinary natural catastrophes. A secondary market might also be created by these contracts, since it was believed that the capital markets would view them as facilitating a market for securitized products.

This concept was adopted by the House Banking Committee, then languished in the House Rules Committee before going to the floor. Congress adjourned before it was enacted, but the conceptual framework was generally appealing to both the government and the private sector.

A more recent idea is for the government to allow companies to set aside reserves for catastrophe exposure—whether acts of terrorism or natural catastrophes, a method currently applied in other countries to help finance catastrophe risk.

The insurance commissioners, through NAIC, have developed a formula for such reserving, but there is resistance from the Treasury and the IRS over providing related tax relief to insurance companies. There is also resistance from the accounting community, which is concerned about the potential manipulation of reserves for contingent future events.

Special purpose reinsurance vehicles are yet another current initiative. The NAIC has adopted model legislation to facilitate the creation of special purpose reinsurers on a state-by-state basis. However, the approach lacks the tax benefit of offshore special purpose reinsurance vehicles and would require changes in federal tax law to be effective.

APPROACHES SINCE 9/11

Ideas for a public-private partnership to finance catastrophic risk in the wake of 9/11 must be examined in light of the concepts advanced over the last decade.

The industry's first instinct after September 11 was to create a pooling mechanism, using the United Kingdom's successful Pool Re program as a model. The industry felt that the sharing mechanism associated with this pool, together with the necessary federal government reinsurance, was a workable approach. It would provide liquidity in a startup period if a catastrophic loss due to terrorism occurred before the pool could become more self-sufficient. The administration, effectively the Treasury Department, was against this. They felt that a pooling mechanism formed by the industry with government backing created a potential monopoly that would stifle private innovation. Treasury preferred to create a mechanism that would result in private sector development of terrorism coverage.

A direct co-insurance program was viewed more favorably by the administration. Under this concept, the Treasury would enter into a relationship directly with consumers, issue contracts—commercial and residential—that included coverage for acts of terrorism, and pay a set percentage of losses for those contracts. The first proposal called for the industry to pay 10 percent, the government 90 percent.

Last fall Congress rejected this idea as unrealistic, saying it put the government directly in the insurance business without adequate compensation.

The House of Representatives has passed legislation providing a role for the federal government in reinsuring acts of terrorism. Under this legislation the industry has a low retention of $1 billion of insured loss. A company retention enables individual companies to benefit from the program. The government provides reinsurance above this amount.

Under this program the government loans money to an insurance company to meet liquidity needs. The loan is paid back essentially through assessments across the commercial insurance premium base. For example, AIG is loaned $500 million; however, it pays back its pro rata share of the commercial insurance marketplace, which may be a higher amount. Whether or not loans were provided, Chubb pays its market share; Hartford pays its share. Every other insurance company in the commercial marketplace would pay its share, without regard to its actual losses or government loans. A percentage of each payment would be paid through a surcharge on policyholders.

While this program passed easily through the House of Representatives, it does not appear that it will have the support of either the industry or the administration. Its passage came over the objections of the administration, and insurers do not welcome a program that would add debt to companies already suffering the financial consequences of a mega-catastrophe.

WHERE WE ARE NOW

In the Senate, meanwhile, legislation currently faces a stalemate. The Senate recently considered a program that had a notional industry retention of $10 billion. Each company would have a retention, effectively 7 ½ percent of commercial lines premium. There would be federal reinsurance above this, along with a statutory cap placing a ceiling on payouts, both for the government and for the industry, at $100 billion.

The administration was active in negotiating this program with a few key senators, and it is still on the table with the current Congress. It has not been enacted largely due to a dispute between Republicans and Democrats over tort reform provisions—something the industry did not push either way.

At the time of writing, the Senate was making some progress toward resolving the tort issue.

NEW IDEAS

Among the new ideas that have received favorable consideration is the auction of excess-of-loss reinsurance contracts, a concept developed by Professors J. David Cummins and Neil Doherty, both of the Wharton School of the University of Pennsylvania.

Under this approach, the federal government would set a reserve price below which it would not sell the contracts. The price would be indexed to aggregate industry capital, and auctioned in the public markets. The idea resonates well with this administration, though it has not been introduced as legislation at the present time.

Another recent concept is for the government to purchase corporate "catastrophe" bonds from the industry. There would be a standing authorization to purchase corporate bonds from companies, which could be treated as contingent obligations by the government.

A third notion is federal reinsurance without basis risk. This would be a government reinsurance program that is directly associated with individual companies and tied to underlying exposure.

One of the more highly publicized proposals is one voiced by New York Senator Chuck Schumer, under which the federal government would assume all risk of loss up to $100 billion from any entity, person, or corporation that cannot get insurance and that has been certified by the state insurance regulator. This proposal has not yet been introduced as legislation, and the industry reaction is that it would do little to deal with the industry's existing exposure. Moreover, it is not clear how losses exceeding $100 billion would be financed. The assumption is that the government would step in. Treasury has told the industry that they are providing a "technical response to Senator Schumer."

LESSONS LEARNED

From these developments it is possible to draw several lessons concerning the possibilities for public-private partnerships. Some of the key points are as follows:

For there to be a public-private partnership, there must be a government nexus. While it has always been difficult to convince the federal government that there is a nexus between government and natural catastrophes, there clearly is a link between acts of terrorism and the federal government. The federal government has undertaken a war on terrorism. In addition, the law enforcement role of government is the primary risk management program for reducing the terror risk.

Basing a program on the certainty of future losses is a difficult sell in Washington. Politicians tend to act when there is an immediate crisis, not in response to projected calamities, and Congress has not been good at getting ahead of the curve in this area.

Risk specific has more resonance. Dealing with catastrophe risk broadly is not nearly as resonant with Congress or any administration as zeroing in on specific risks, whether they are acts of terrorism, hurricanes, or earthquakes.

Any suggestion of tax advantages for the insurance industry is an extremely tough sell. While one could make the case that special purpose reinsurers need a tax exemption or tax deferral in the United States in order to bring special purpose entities onshore, the Enron debacle has tainted special purpose entities as creative financing techniques—making them a difficult sell.

The industry must have "skin in the game." If the industry does not retain some risk, the government will not share the risk.

Government has its limits. The government does not have the appetite to take on insured terrorism risk for any extended period of time or to pay for unlimited losses.

The government is not going to do anything that does not lead to an ultimate private sector solution.

The government will serve as a backstop, not a "stop and shop" for consumer insurance coverage.

There are no viable solutions for basis risk in the public-private partnership domain. The government prefers a generic, not a company—specific role.

Any proposal—whether for natural catastrophes or terrorism—will not be used as a means to achieve federal regulation of solvency, rates, or coverages.

Loans and grants to the industry are a non-starter with Congress. Premiums must be part of the package in some creative way.

The industry has unlimited risk and limited capital. The capital base of the commercial insurance market in the United States is about $130 billion. This does not include companies that are primarily personal lines markets, which account for an additional $170 billion. The terrorism exposure dwarfs these figures. Considering the full spectrum of workers compensation, property, cyber, and other exposures, the risk is extraordinary. And it is a risk that will be with us for a long time. The industry must find a role for government in capping its exposure or financing its exposure over time.

There need to be better private sector solutions at the end of any government program or as part of any government program.

Last fall, there was unanimous industry agreement that the terrorism risk be addressed with a pooling mechanism. The industry was flexible and supported various approaches. But the industry faces a "prisoner's dilemma," in which entities operating in their own self-interest tend to undermine the interests of the whole.

Ours is not a monolithic industry. Companies that focus primarily on workers compensation see the issues differently from companies that are largely personal lines underwriters. Commercial lines carriers see it another way, while reinsurers have a wholly different perspective. The different and sometimes conflicting interests of these various constituencies challenge the effectiveness of the whole in finding a solution.

The message from Congress and the administration is that insureds —or those unable to get terrorism insurance—must make the case for government participation in these risks. Some, like the real estate community and mortgage bankers, have been fairly active on the subject in Washington.

The government needs to recognize that the problem is nationwide. It affects the financing of economic activities not only in New York but throughout the country. Many different entities across the nation are seeking insurance for acts of terrorism and are not satisfied with the coverage currently available or with the exclusions that apply. To address this widespread and growing problem, some program must be established that gives insurers some certainty over total exposure.

CHAPTER 5

Managing the Risk: The Marsh Perspective on the Terrorism Market

Julie A. Martin
Vice President, Marsh

This overview of Marsh's perspective on the terrorism market spans:

- types of terrorism exclusions on property cover
- requests in the United States for stand-alone terrorism cover and factors affecting premiums for such covers
- current markets for stand-alone cover
- the future for property terrorism risks

TERRORISM EXCLUSIONS IN PROPERTY INSURANCE

Marsh has identified at least 17 different types of terrorism exclusions on property insurance policies. Most contain a broad definition encompassing all or some of the following conditions:

- an individual or a group
- acting alone, on behalf of, or in connection with any organization or government
- committed for political, religious, ideological, or similar purposes
- with the intention of influencing any government and/or putting the public, or any section of the public, in fear.

Many exclusions may be interpreted to omit certain acts or losses previously covered, such as vandalism, malicious mischief, riot, and civil commotion. This has led to some mismatch between the stand-alone terrorism policies that are being bought back and the exclusions that are in place.

Some terrorism exclusions expressly exclude the use or release of chemical, biological, or nuclear materials, but all of the wordings essentially encompass this intent. The burden of proof regarding whether or not an event is an act of terrorism lies with the insured.

Buyers of terrorism coverage are primarily Fortune 1000 companies and run the full gamut of industries.

REQUESTS IN THE UNITED STATES FOR STAND-ALONE TERRORISM COVER

There is a large amount of market activity in the area of stand-alone terrorism cover. Marsh is currently working on approximately 150 different requests for stand-alone terrorism cover in the United States, and we have seen many more than that.

To date, about 15 percent of the requests Marsh has managed elected to purchase cover, while another 15 percent of clients declined to purchase cover. One of the reasons cited early on for not purchasing coverage was the potential for federal action. Those forgoing coverage also cited what they perceived as expensive pricing on coverage that had in the past been "thrown in" to the property program for free or for a minimal cost.

Since January 1, 2002, when Congress adjourned without passing any kind of backstop program, risk managers have become more skeptical about the United States government's ability or willingness to provide a solution, and coverage requests and purchases have increased.

The remaining 70 percent of the clients seen by Marsh are still in the process of deciding whether or not to pursue terrorism coverage. No client, regardless of reported risk, has been declined a quote, although some quotes have come with numerous exclusions.

Potential Buyers

Buyers of terrorism coverage are primarily Fortune 1000 companies and run the full gamut of industries. They include real estate companies with "trophy" buildings and properties, as well as bridges, stadiums, and large office buildings.

Properties located near potential targets (e.g., the area surrounding the White House) represent another group of buyers. Banks require coverage both on their own account and as project lenders. Construction projects, hospitals, hotels, media, energy, and mining operations are other examples of the wide range of potential buyers.

Insurer Responses to Stand-Alone Terrorism Requests

Limits on stand-alone terror coverage have been set between approximately $5 million and $350 million. Most frequently they fall into the $25 million to $200 million range. Deductibles or self-insured retentions range from approximately $50,000 to $50 million for property losses, but remain most often in the $1 million to $5 million range. This has been in large measure because primary property insurers have been providing sublimits at that level, and coverage has been placed on top of that. The deductible for business interruption coverage has typically been 30 days.

Annual premiums have been wide-ranging, from $55,000 to $15 million. Rates initially varied significantly from approximately 1 percent to 10 percent on the limit of cover requested. However, since February rates seem to have declined to about .04 percent to 2 percent on the limit of cover requested. Those rates, however, are significantly affected by the particular risk being quoted. If it is a high profile or "target" property or a large-value exposure, pricing can be significantly higher.

FACTORS AFFECTING PREMIUM

Pricing is very client specific, though there are several factors driving premium, including the values declared and the limits requested.

As more entrants come into the market, larger amounts of coverage are being placed. The additional amounts, however, may become more expensive.

Deductibles and self-insured retentions also impact premium. Deductibles under the property policy are no benchmark; deductibles are generally much larger in the terrorism market. Premiums are higher for non-cancelable versus cancelable policies. A target or trophy risk (e.g., a bridge, tunnel, or conspicuous office building) will also increase premium.

Whether or not underwriters have aggregation of exposure at a particular location also affects premium. Many underwriters are starting to have aggregation in Manhattan, Chicago, and Washington, D.C. Companies looking to place a risk in these areas will find coverage more expensive.

Location affects premium. Factors include whether the risk is in a city center or a rural area, whether it is a single or multiple location, and whether it is in a country considered high or low risk. Risky locales used to mean such places as Southern Algeria or Colombia. Now being located in the United States will often raise the price.

In many instances, exposures have been separated, with some placed in existing government programs, such as those in the U.K. or South Africa, in order to obtain a blended rate that is possibly more economical.

Factors such as a facility's security, terrorism loss history, and the nature of occupancy are also considerations. The risk is considered greater, for example, if a government agency resides in a building.

As information on pricing and limits continues to emerge in this rapidly changing market, Marsh has begun developing a database to give potential buyers a sense of pricing. As they get a sense of the pricing, many potential buyers are opting not to pursue coverage.

THE MARKET AFTER 9/11

Total capacity after the World Trade Center attack has varied, but is in the range of approximately $200 million to $500 million, depending on the risk, the market appetite, and the premium tolerance of the client.

Perhaps the biggest question is: What impact will the next attack have on the market?

There are essentially four markets:

- Lloyd's, which currently ranges from approximately $50 million to $150 million per risk.
- AIG, through Lexington, which is in the $50 million to $150 million range.
- AXIS Specialty, which ranges from $50 million to $100 million.
- Berkshire Hathaway, offering from $50 million to $200 million in capacity.

Allianz has formed a consortium, which is still in its embryonic stages, but is expected to begin writing soon.

KEY ISSUES WITH STAND-ALONE COVERAGE

Major issues with stand-alone terror coverage include:

- The "mismatch" that exists between the exclusions in property policies and the stand-alone terrorism coverage that can be purchased back. This mismatch creates gaps. For example, under stand-alone property terrorism policies, cover is provided for direct physical damage and physical loss; exclusions may address threatened or consequential damage, creating a possible gap.

- The war exclusion creates a similar potential lapse, and there is no cover for nuclear, chemical, or biological releases or for cyber terrorism.

- There is a non-concurrency between the Lloyd's T3 form and AIG's stand-alone terrorism forms, which can make it difficult to provide seamless layers of coverage.

- Coverage for business income, extra expense, and loss of rent —all excluded from terrorist acts under property policies— may not be available to be repurchased fully.

- Structuring terrorism programs is complicated. The aggregate limit cannot be reinstated and only covers specified locations. Exact street addresses of all locations worldwide must be provided so that underwriters can track aggregates in various places and specific locations. It is critical that declared values and schedules be accurate.

- Cancelable versus non-cancelable coverage is a concern. AIG is the only market that currently does not offer a non-cancelable policy. However, securing a policy that is non-cancelable from other markets, such as Lloyd's, would perhaps affect pricing.

THE FUTURE

Today there are more questions than answers about the future of property terrorism coverage. Perhaps the biggest question is: What impact will the next attack have on the market?

The current providers of stand-alone property terrorism cover will be unable to meet the significant demand of both owners and lenders. Will there be a United States government initiative? If so, how much additional capacity will it mobilize? There is also the potential that other government schemes will be developed. One was recently developed in France, and another is being launched in Germany.

Will reinsurers provide terrorism coverage again in property policies? Or will it be a stand-alone reinsurance coverage for the future? How will clients view self-insurance? Many insurers are assessing the cost-benefit. Industry captives are also being explored, though at a nascent stage. The industry must also begin to address liability exposures arising from terrorism.

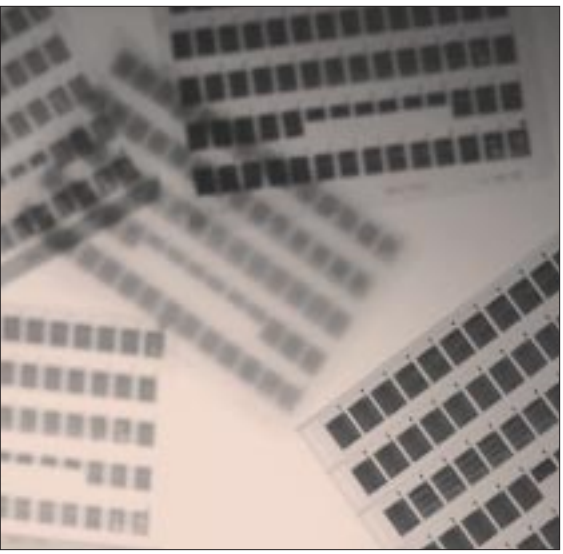
Finally, even if there is a United States government program, a huge gap will continue to exist for many emerging markets and international locations, because most of those insurance companies turn to the same reinsurers.

There are no answers to these questions today. However, the market has been dynamic, responding relatively quickly after September 11 to provide some solution. Now the industry must forge ahead toward an even greater solution for managing the risk of terrorism.

CHAPTER 6

Cyber Risk: Is Terrorism the Biggest Threat to Your Business Community?

Mary N. Guzman
Senior Vice President, Marsh



Is terrorism the biggest threat to your organization? From a cyber-risk perspective, probably not. The risk of cyber attack is not much different now than it was before 9/11. The motives behind an attack are not necessarily relevant for the purposes of insurers and reinsurers. Whatever the motivations, a cyber attack can still have the same effect on a company's business continuity, on its supply chain, or on its ability to service customers and vendors.

MISCONCEPTIONS ABOUT E-RISK

There are many misconceptions about cyber risk. The most common is that you don't face much risk if you are not using your Web site to provide e-commerce solutions to your customer base.

Nothing could be further from the truth. Your network has just as much to do with your exposure as the Internet, possibly more. A company's network typically houses information and systems that are essential to such key activities as employee benefits administration, shipping/receiving, accounts receivable/payable, warehousing, logistics and supply-chain management, and strategic business practices, such as pricing and competitive analysis. The Internet is simply the portal that hackers use to get to the critical systems that are behind the firewalls and "DMZs."

Therefore, even if a company does not move products or services over its Web site it can still suffer a tremendous loss from a major cyber catastrophe.

A second widespread misconception is that using a firewall and anti-virus software will make your information secure. A firewall is not going to protect you from, for example, certain viruses that ride in on e-mail. Businesses must leave their networks open to some vulnerabilities in order to do business. Port 80, the port through which Web traffic passes, is a perfect example of this.

A security assessment firm may be able to identify particular vulnerabilities on a company's network, and they may be able to recommend ways to remedy the problems. But there are certain vulnerabilities that simply cannot be corrected if the network is to continue operating.

Cyber risks fall into three major categories: liabilities to third parties; property loss; and crime.

Moreover, certain attacks have nothing to do with firewalls, and everything to do with network security architecture and load balancing. An example is a distributed denial of service (DDOS) attack, in which a hacker goes into somebody else's network, puts a Trojan horse on the server, and uses that server as a proxy to launch an attack against another party. These attacks are not prevented by firewall capabilities, because they involve legitimate requests at the Web site, but there are just too many requests for the server to handle.

The effectiveness of anti-virus software is limited as well, since such software can only prevent known viruses.

Many issues related to cyber security have nothing to do with technical vulnerabilities or technology itself. The fact that most professionals in our industry can access the Internet from their desktop illustrates the security risk organizations face.

CYBER RISKS

Cyber risks fall into three major categories: liabilities to third parties; property loss; and crime.

Liabilities to Third Parties

Liability risks take several forms. One that has received much attention lately is the privacy issue, which includes theft of personal information, such as bank records, as well as identity theft in general. There are currently a number of legislative and regulatory efforts aimed at making organizations responsible for the privacy of their customer information. This is a "hot button" issue for the United States government and will continue to gain importance.

Other growing areas of liability include content risks, such as intellectual property exposures, and liability for Internet "wrongful acts," when a company's system is used to attack others.

Third-party liabilities also arise from contractual violations and delays in delivery that impact a company's supply chain. For example, if a company's system is interrupted, or if inventory or shipping data is corrupted and becomes unusable, the company may be left unable to meet its contractual obligation to deliver a product.

Property Loss

First-party property losses stem from the direct loss of data and typically involve losses due to business interruptions.

Property policies—even before 9/11 and before carriers began specifically excluding viruses—did not respond to DDOS attacks and other "loss of use" claims. In these cases there is, technically, no damage to or direct loss of a tangible asset, which is what property insurance is designed to cover.

Crime

Crime exposures include cyber-related theft of information assets and cyber vandalism. Cyber extortion is also a continuing trend. These threats may take the form of a demand for money in exchange for not releasing information about a company's customer base or perhaps a hospital's patients.

Companies may also face liabilities as a result of crimes or malicious acts perpetrated against others using their company system—which may be one of the scarier security liability risks.

Contingent Exposures

Contingent exposures are another big issue in the cyber world. The concept of hosting is an example. Credit card and other Internet transactions are often processed by someone at a site other than the site being visited—often unbeknownst to the customer. Hence companies are exceptionally reliant upon those hosting their Web site, hosting a critical application, or providing a major technology service. Yet the vast majority of the contracts that hosting or application service providers (ASPs) issue to their customers state that the hosting company is not responsible for any consequential damages, any punitive damages, or any monetary damages at all.

This issue becomes particularly critical for time-sensitive businesses, such as companies whose customers buy and sell stock over its Web site. If the Web site is unavailable for four hours, the Nasdaq is plummeting, and customers are unable to trade stock, the company not only loses potential commissions, it could face serious liability lawsuits from its customer base.

Besides having no contractual responsibility, ISPs and ASPs are often not economically able to handle a major loss they may cause. One troubling scenario might involve a disgruntled employee who maliciously launches a DDOS attack or a virus against the hosting company's entire customer base. This raises aggregation concerns for insurers and reinsurers.

The good news is that the risk truly can be managed if you understand what the risk is and are willing to invest in security technology, policies and procedures.

The Internal Threat

More than half of all cyber attacks are perpetrated by a company's own employees or contractors. This is a huge security issue, for in many cases the attacker is already behind the firewall, with authorized access to critical information.

WHAT IS AT STAKE?

Cyber attacks and other cyber losses can cost a company its reputation and the trust of its constituents or customer base. This is particularly sensitive for financial institutions and other companies whose entire business is based on trust.

Companies can lose their ability to service customers or distribute products through vendors.

Companies can also lose strategic information, such as trade secrets, which raises a further issue. Trade secrets are not technically protected under intellectual property

Chances are, only the top 10 percent of the leading 2,000 United States companies (by revenue) could even come close to a perfect score on a network security assessment.

rights, but they can be covered under cyber-risk policies, if they can be valued. How to value them is a problem now being considered by companies. One suggestion is to find out what internal auditors are doing with the accounting firms to value such information for financial purposes. This may lead to some consensus regarding the value of trade secrets under cyber-risk policies.

Yet another consequence of cyber attacks involves the violation of customers' or constituents' privacy. In addition to the enormous negative impact on a company's reputation, such violations of privacy can also affect the stock price of publicly traded companies. Down the road, class action liability suits may arise when a company's stock price drops as the result of a security breach.

SECURITY MANAGEMENT CHALLENGE

The best technology in the world still relies on people to implement it properly. Security talent is hard to find. And it is expensive. It is difficult to keep up to date with the latest hacking events and viruses.

As a result, most companies have limited cyber security. Chances are, only the top 10 percent of the leading 2,000 United States companies (by revenue) could even come close to a perfect score on a network security assessment. These assessments are very challenging. At Marsh, we encourage our clients to invest the resources needed to develop the best possible technology security, processes, and procedures.

Changing the Security Management Mindset

There needs to be a change in the mindset of senior management with regard to security management. Management needs to understand that no "silver bullet" technology is going to prevent cyber attacks from occurring across the board. Viruses cannot be prevented unless the particular strain of virus has been seen before. Anti-virus software only combats known vulnerabilities in a system. The only way to prevent a DDOS attack altogether is to unplug the server.

But losses can be mitigated, and many things can be done from a security perspective.

Companies have the choice of managing security themselves—which can be expensive and difficult—or outsourcing. Many opt for a combination of both.

CYBER RISK AND EXISTING INSURANCE POLICIES

Traditional insurance policies do not adequately address cyber risks.

Property policies are designed to cover direct losses of tangible assets, not indirect losses of intangible assets. Even if a loss is determined to be covered, the valuation clause is a problem. Intellectual property stored electronically is valued as "data," not as revenue, therefore business interruption coverage is not triggered.

Concerns over third-party coverage include the fact that many companies do not have E&O coverage. Even if they do, the policy may exclude security breaches and certainly excludes intentional acts on the part of the insured, which is a problem since more than half of all hacking events are committed internally by employees.

Advertising injury coverage under general liability policies does not adequately address intellectual property infringement, content or advertising offenses perpetrated over the Internet, including invasion of privacy or identity theft.

Nuances in many crime forms do not extend coverage to theft of information assets. Moreover, they often require that there be a personal profit motive in order for the offender to be prosecuted, or they may trigger coverage only when the offender is a current employee.

Kidnap, Ransom & Extortion policies are designed to cover threats of bodily harm.

TERRORISM EXCLUSIONS ON CYBER-RISK POLICIES

Many carriers are currently developing terrorism exclusions for cyber-risk policies, but issues unique to cyberspace make this an unusual frontier. Some of the key problems to be considered in this respect include the following:

- A good "hacker" can cover his tracks and can launch an attack from anywhere in the world.
- Forensic capabilities are very good, but it is still difficult for carriers to prove that an attack was an act of terrorism or war.
- Cyber policies are explicitly designed to cover intentional malicious acts launched against a network.
- The burden of proof, from a liability perspective, is on the insurer.
- Good policies provide a duty to defend until final adjudication.

THE STATE OF THE CYBER-RISK MARKET

The state of the cyber-risk market has not changed significantly since 9/11, except for a rise in premiums. Some issues of capacity are arising with regard to "critical infrastructure" organizations, particularly financial and healthcare institutions. Marsh believes that $200 million in capacity can be found today for any one risk.

Six key carriers offer primary cyber-risk coverage today. They include AIG, Chubb, and Zurich in the United States, as well as Lloyd's syndicates. These carriers will fill out the first $50 million on a risk, the most difficult layer to fill. Ace, XL, and a number of other carriers will sit over $50 million.

Stand-Alone Policies

Why have stand-alone cyber-risk policies not yet taken off? In fact,

they have, compared to this time last year. But cyber-risk coverage involves an education process analogous to that seen when employment practices liability (EPL) insurance was first introduced. EPL policies were rarely purchased in those early years, though there was much discussion about them. Then, with the first punitive damage award in an employment practices case, the floodgates were open. Today, the vast majority of Marsh clients purchase an EPL policy.

The cyber-risk issue is similar. Most companies have liabilities in this area, though some have more severe exposures than others. It is not a lack of exposure that is impeding policy sales. Some of the reasons for the slow growth of cyber-risk policies include the following:

- P&C carriers have been slow to adopt an affirmative position on coverage for cyber risk.
- Clients continue to have misconceptions about the quality of their network security and about their Internet liability risks.
- Though there have been many viruses that have cost companies billions of dollars, companies continue to have difficulty valuing business interruption claims.
- The United States has not experienced any substantial cyber-liability awards that include punitive damages. Therefore, corporations and directors and officers do not feel vulnerable—especially since there has been no agreement on a "security standard" against which liability is measured.

THE FUTURE OF CYBER-RISK POLICIES

All of this is going to change. Insurers have already started to clarify policy language. Companies are beginning to feel pressure from shareholders and regulatory agencies to prove that they have adequate security.

And for the first time there is an ISO standard for network security, ISO-17-7-99. This arose from the British standard, 77-99. Underwriters often use this standard when they send security firms to assess a company's network security. The new standard raises the bar in terms of the security that companies will be required to have, and it gives plaintiff attorneys the ability to establish negligence.

Ultimately, things will change, because for every million dollars in revenue, companies spent just $239 on IT security in 2000. This number rose to $316 in 2001 (Yankee Group, 2001). That is still a miniscule percentage considering the risks—a percentage that would make it easy for the federal government or a plaintiff's attorney to make a solid case against a company for negligence in network security.

CHAPTER 7

PANEL DISCUSSION: Insurance and Reinsurance Solutions for Cyber Risks

MODERATOR

Harrison D. Oellrich

Managing Director, Guy Carpenter & Company, Inc.

While cyber risk may not be entirely "on message" for a conference focused on the broader issue of terrorism, there are aspects of emerging cyber exposures that can be defined as cyber terrorism. These emerging exposures are here to stay, and the insurance and reinsurance sectors must develop responses if e-commerce is to reach its tremendous potential.

The sophisticated exposures associated with cyberspace were never contemplated in the past, and as they have grown in recent years, insurers and reinsurers have become increasingly concerned that they cannot be successfully underwritten, at least not within the context of traditional "brick and mortar" property and casualty forms. Unlike traditional property and casualty exposures, many cyber risks are intangible. Yet if a company's confidential electronic information is disclosed, lost, stolen, destroyed, or corrupted, the impact on earnings and even on share price can be very tangible indeed. And it can occur within hours, not days or weeks.

Recognition that these exposures are significantly different further fuels concerns on the part of reinsurers that ceding companies are not sufficiently able to quantify, underwrite, and price them, particularly when they are underwritten as part of existing policies.

Consequently, reinsurers are in the process of mandating that loss from certain of these new exposures—especially worms and viruses—be tightly controlled, if not entirely excluded, within the traditional portfolios they reinsure. This process was well underway prior to 9/11, and will be reemphasized as insurers and reinsurers negotiate and renew existing agreements in the coming months.

The result for most businesses is that coverage for cyber risk is being dramatically curtailed, if not eliminated entirely, in existing property and casualty policies. As businesses grapple with this reality, a new generation of stand-alone insurance products focusing solely and specifically on cyber exposures has been developed and is already undergoing refinement.

Begun several years ago with foundation-building work by our primary insurance colleagues at Marsh with their NetSecure product, AIG's NetAdvantage Suite, Chubb's Cyber-Security for Financial Institutions, Zurich's E-Risk Edge, and other products have subsequently been developed to provide specific solutions for companies transacting business over the Internet. Since these are stand-alone products, they allow underwriters to assess, underwrite, and price each insured's unique Internet exposures—which in turn should make covering cyber exposures more attractive to prospective reinsurers.

In this chapter, four experts in the field of cyber risk will explore the topic of insurance and reinsurance solutions for cyber risks in greater depth.

INSURANCE COVERAGES FOR CYBER RISKS

Jeffrey S. Grange
Vice President,
Chubb Department of
Financial Institutions

Reinsurers are thoroughly familiar with the universe of natural and man-made threats, including collapse, flood, tornado, hazardous spills, ice storms, and the like. But what are the business impacts of a massive service disruption due to a network security failure?

As companies migrate more and more of their core business processes to Web-enabled networks, they become increasingly vulnerable to cyber attack, including cyber terrorism. Vulnerabilities include widespread service disruptions, system shutdowns, and business interruptions.

In many "old economy" businesses today there is a growing dependence on information technology in manufacturing, scheduling, logistics management, inventory controls, and sales functions. Business models are increasingly reliant upon digital control systems, single-source suppliers, just-in-time inventory management, and key ISPs and ASPs—information technology and telecommunications backbone providers.

Have insurance and reinsurance underwriters done a sufficient job of identifying the vulnerabilities of these networks, assessing the probabilities of threats to these business models, and quantifying the potential business impacts? Insurers and reinsurers must remain relevant to their customers, and an efficient risk transfer market for cyber risk is vital to meeting the risk management needs of customers in the years ahead.

Key Concerns

In Chubb's market research, 76 percent of bank directors identified e-commerce risk or cyber risk as their number-one risk management concern going forward. Eighty percent of these directors think they have already "got it covered" under traditional insurance programs.

Customers and regulators are primarily concerned about four issues: privacy, service disruptions, disaster preparedness and business continuation planning, and the growing dependence on outsourcing.

Customers and regulators are primarily concerned about four issues: privacy, service disruptions, disaster preparedness and business continuation planning, and the growing dependence on outsourcing.

Managing Cyber Risk

The emerging risks of electronic commerce should be segregated from traditional primary insurance covers because the volatility of the emerging risks of electronic commerce could potentially wipe out available insurance for traditional categories of event risk. Insurers and reinsurers must generate new premium revenue streams to pay for future losses arising from the emerging risks of electronic commerce. The alternative is to cannibalize even further traditional premium revenue streams that are demonstrably lacking from a rate adequacy perspective.

Education and awareness about the emerging risks of electronic commerce are key priorities, and insurers are investing heavily in these areas.

Cyber risk represents an important risk management challenge for the future. To address it, we must break down the barriers and the functional silo mentality that exists today between line departments, such as traditional risk management, security, information technology, finance, human resources, legal, and the like.

Information security is not simply an IT problem. It is a line-of-business issue and a risk management issue. And because of the real-time reputation risk, it is a corporate governance issue as well.

It is vital to quantify the bottom line monetary cost of information security failures at both an enterprise and a systemic level. Quantification of cyber risk will permit the efficient allocation of scarce IT security resources to defend against those known vulnerabilities that concern companies most.

A "total cost of risk" approach will also identify those cyber risks that are highly diverse, infrequent, catastrophic, and therefore most appropriately transferred to third-party insurers and reinsurers. Since our physical and cyber infrastructures are only as strong as the weakest link in this highly interdependent network chain, it is important that companies forge partnerships with one another, as well as with federal, state, and local governments and law enforcement. Working together, we will be more successful in understanding and identifying known vulnerabilities, and in managing the ever-expanding universe of cyber threats, including cyber terrorism.

Chubb has long believed in such partnering and has forged relationships with key leaders in government, law enforcement, academia, and the reinsurance community to tackle cyber crime and cyber terrorism around the globe.

The risk of cyber attack is as bad as you think it is, and possibly a lot worse.

INSURANCE AND RISK MANAGEMENT SOLUTIONS FOR CYBER RISKS

Ty R. Sagalow
Executive Vice President and Chief Underwriting Officer, AIG e-Business Risk Solutions

AIG formed AIG e-Business Risk Solutions in January 2000. Today, it is a dedicated unit with over 50 members and a simple mission: to evaluate the risks of the New Economy and design solutions combining risk management advice, technology, and insurance.

AIG e-Business Risk Solutions is the world's largest provider of network security insurance, with over 1,500 past and present AIG netAdvantage clients. Many other insurance companies are forming their own e-business risk units.

The Risks

The risk of cyber attack is as bad as you think it is, and possibly a lot worse. According to the CSI/FBI 2001 Report, 85 percent of companies reported at least one successful computer attack. Ninety percent of those companies say they have a working firewall. Some 64 percent have acknowledged financial losses due to cyber attacks, with an average financial loss of approximately $2 million per attack.

There have also been the so-called "mass cyber events" over the past several years. Events such as NIMDA, estimated to cost $500 million; Melissa estimated at $80 million; the Love Bug estimated at $10 billion; the two Denial of Service attacks of February 2000 that some tally at $1.2 billion; and Code Red, which affected more than 200,000 computers. These loss estimates are not necessarily reliable numbers, but they are the numbers that security experts refer to repeatedly. However precise or imprecise such figures may be, the fact remains that the problem is big—very big.

So, how can it be managed? Technology alone cannot eliminate security risks: there is no single "magic bullet."

Firewalls will not stop a denial of service attack. Anti-virus software is only effective against known viruses, and will not be effective against first attacks by a new virus. While they are all worthwhile technologies, intrusion detection, access control, encryption, and even public key infrastructure will not stop the bad guys forever. Nor can insurance alone sufficiently mitigate the security risks.

The Total Risk Management Approach

AIG strongly recommends a total risk management approach—a combination of best-in-class technology, people, processes, procedures, and insurance. This approach is in line with what many are calling the cyber-risk management cycle.

The cycle begins with a security risk assessment. Many insurers

AIG netAdvantage Suite

COVERAGES	netAdvantage	netAdvantage Professional	netAdvantage Liability	netAdvantage Security	netAdvantage Complete
Web Content Liability	●	●	●	●	●
Professional Errors and Omissions		●	●		●
Network Security Liability			●	●	●
Cyber Extortion			●	●	●
Network Security Property Loss (Intangible Information) (1st Party)				●	●
Network Security Business Interruption Coverage (1st Party)				●	●
Cyber-Criminal Reward Fund				●	●
Crisis Communication Management Fund				●	●

Source: Ty R. Sagalow

provide free online security assessments based upon British Standard 77-99. Many also provide complimentary site security assessments under certain circumstances. Some of these onsite security assessments are available from the insurance industry regardless of whether insurance is purchased.

The next phase of the cycle is to mitigate the risks revealed in the assessment, and where those risks cannot be mitigated to insure the exposure. Since it is not possible to prevent all attacks, the cycle also calls for detecting an attack, recovering from the attack (including insurance recoveries), then remediating and starting all over again with a new reassessment of the security risk. The cycle is an ongoing process of improvement.

Choosing an Insurance Partner

When selecting a partner to insure cyber risks, consider the following criteria:

- Experience: require a carrier to have a minimum of two years with a dedicated unit addressing cyber risk.
- Financial strength: seek S&P ratings of AA or AAA.
- Global reach: look for global operations that are actually owned by the insurer.
- Insurance capacity: should be a per-policy minimum of $25 million.
- Robust loss prevention services: ascertain whether top quality third-party providers and educational materials are used.
- A dedicated e-business risk structure: which should include underwriters, claims specialists, legal professionals, and technologists with worldwide authority over all company units and divisions.

What should you look for in a best-in-class program? First, loss prevention services, which should include free or discounted assessments, along with security services and products. One should also be sure that the program has broad insurance coverages, including coverage for:

- Third-party liability
- Media related risks
- Professional errors and omissions
- Third-party security risks
- First-party property and business interruption
- Cyber extortion

In addition, look for post-incident support funds, such as funds to pay for public relations consultants to explain to employees, shareholders, and customers why the cyber event was not as bad as they may have heard elsewhere.

Whether it comes from AIG, Chubb, or another carrier, cyber-risk coverage is critical. Look for the right carrier and the right program.

INTERNET LIABILITY INSURANCE: THE STATE OF THE REINSURANCE MARKET

Sandy G. Hauserman
Senior Vice President,
Guy Carpenter & Company, Inc.

Before insurers can take full advantage of the potential represented by the explosive growth of the Internet, there must be a viable reinsurance marketplace to support their efforts. No primary insurer will venture into such a new and untested arena—where recognition of the client's exposure is ongoing and coverage grants and rates are quickly changing—without the help of reinsurance partners.

Internet exposures are sophisticated and in many ways different from traditional "brick and mortar" exposures because they are mostly intangible. Many Internet exposures were never contemplated nor covered within traditional property and casualty policy forms. In addition, reinsurers have concluded that what coverage may exist in traditional property forms is exceedingly difficult to quantify, underwrite, and price. As a result, reinsurers are in many cases dramatically curtailing—or eliminating entirely—all Internet coverages in reinsurance programs protecting such policies. This process has helped to foster the development of stand-alone policies, like AIG's NetAdvantage Suite, Chubb's CyberSecurity for Financial Institutions, and Zurich's E-Risk Edge, which focus specifically on Internet exposures.

In order to help the Internet liability marketplace grow and mature, Guy Carpenter has been active in helping several insurers find quota share support for their policies. The reinsurers from which we have solicited support have undertaken extensive due diligence to vet policy offerings and understand the nature of the exposures presented. This has led to the growth of a small but knowledgeable group of reinsurers that understand this business.

As part of the vetting process, both reinsurers and insurers have concluded that companies must have a comprehensive security plan in place prior to going online. In addition, there is general agreement about the need to conduct a security assessment prior to binding coverage. These are often done by professional third parties and are seen as a valuable tool to help uncover and address vulnerabilities in an insured's network security protocols.

Finally, redundancies in key systems and a well-thought-out recovery plan are vital to mitigate damage and economic loss in the event of attack.

Despite all of the work that has been done to understand cyber exposures, the reinsurance marketplace has been slow to develop.

Despite all of the work that has been done to understand cyber exposures, the reinsurance marketplace has been slow to develop. Overcoming the steep learning curve to understanding this business requires a significant investment of both time and money.

In addition, as the reinsurance market hardens, many reinsurers are reluctant to apply capital to a new and untested line of business that is difficult to price and that has unknown loss potential. Finally, reinsurers and insurers fear that massive losses, especially business interruption losses, are possible from a single Internet attack.

Because the Internet is so interconnected, there is the perception that a single attack could potentially affect many thousands of businesses across many different networks. Such a massive loss would affect the economy much as a catastrophic hurricane or earthquake would. As a result, Guy Carpenter has dubbed this exposure "Cyber Hurricane."

Cyber Hurricane

To help overcome the reluctance to write Internet liability, Guy Carpenter has developed a Cyber Hurricane catastrophe product, which allows insurers to spread the risk of massive Internet loss. The product will potentially be available from traditional property catastrophe reinsurers.

The first goal in developing Cyber Hurricane was to find a way to divide the Internet so that catastrophe reinsurers could achieve a spread of risk similar to that which exists in their traditional property business.

At first this seemed difficult, if not impossible. Whereas losses from natural perils occur in specific geographic locations, the Internet is both everywhere and nowhere at the same time. On the surface at least, the Internet does not seem to be susceptible to such division.

After much work, we believe we have solved this problem. Furthermore, we have validated our concept by placing the first Cyber Hurricane Catastrophe Cover, supported by most of the worldwide property catastrophe leaders.

Nonetheless, this product will not become widely available unless we can provide a framework for reinsurers to model Internet exposures so that they can quantify their potential for loss and price this product.

Insurers and reinsurers have spent a tremendous amount of time and resources over the last decade attempting to quantify their actual expected losses from just about any physical peril using sophisticated modeling tools.

Data to populate models for "brick and mortar" property catastrophe exposure is plentiful, while

The security requirements mandated by insurers and reinsurers will help the country to protect itself from future cyber attack.

historical data to build and run future models for Internet exposures is virtually nonexistent. In fact, many past cyber attacks have not been reported at all since companies are fearful that sharing such information could adversely affect their reputations.

Toward a Sustainable Marketplace

With credible data and a way to model Internet exposures, there is every opportunity to build a substantial and sustainable reinsurance marketplace. To that end, Guy Carpenter has been working closely with various agencies of the executive branch of the federal government, including the White House, as part of a joint public-private effort to strengthen network security.

Since the government utilizes the Internet in much the same way as the private sector, the Internet has been designated as a key component of America's critical infrastructure, which must be protected from attack at all costs.

Consequently, we believe that we may soon have access to data gathered by various government agencies, and we may even have the opportunity to explore with these agencies the methodologies they use to model these exposures.

Although the Cyber Hurricane product is in its infancy, Guy Carpenter is enthusiastic about the support such a product can provide to the development of a stronger, more robust primary insurance market for Internet liability insurance.

In the meantime, Guy Carpenter believes that building an Internet liability market is critical. Soon, nearly every business in the world will have a Web site and many of these companies will be using the Internet to buy and sell their goods and services. The insurance industry must respond to the needs of its clients and have products available as one of several ways a business can spread its risk of loss. This is the role insurance has always played during times of innovation, and will surely play again in this new arena.

As the insurance industry responds to this challenge, an additional benefit will emerge: The security requirements mandated by insurers and reinsurers will help the country to protect itself from future cyber attack.

PRIVATE-PUBLIC PARTNERING ON CYBER RISKS

Lee M. Zeichner
President, LegalNet Works, Incorporated

The insurance and reinsurance sectors are uniquely positioned to work in partnership with the government to address three important areas of the risk

environment after 9/11. Each of these impacts how your sector will be positioned to underwrite risk and improve the security posture of the nation's business community:

- Risks that are unique to government.
- Risks that are unique to industry.
- Risks that are shared between public and private sectors.

The first area involves risks that are traditionally and uniquely governmental. There are policies and programs in our country for addressing national defense, border control, law enforcement, intelligence, diplomacy, and catastrophic response and recovery, just to name a few. We expect our government, whether at the federal, state, or local level, to address these risks on behalf of all citizens. These are unique governmental responsibilities, risks which no single company or sector of the economy can manage alone. Tradition, history, and constitutional government support exclusive government involvement in these areas.

What has changed with regard to governmental responsibilities and national risk management after 9/11? As a preliminary matter, the government must begin to define national defense responsibilities that involve privately owned critical infrastructure facilities, such as those in banking, healthcare, electric power, and transportation. Everyone can understand that national defense includes deployment of troops overseas to fight the war on terrorism; a more complex question is the extent to which national defense responsibilities also include government contributions to protect critical infrastructure assets here at home. One example is what role the federal government might play in response and recovery on behalf of industry in the aftermath of an attack—a question ripe for public-private dialogue. How, for example, would the federal government respond if terrorists targeted one particular sector, overwhelming the ability of private resources to handle the attack? Would national defense responsibilities depend on which sector of the economy was under attack, distinguishing between an attack on, say, telecommunications as opposed to a less critical sector?

During preparations for Y2K, the federal government grappled with the following scenario: If confronted with a massive and prolonged blackout in Chicago during the middle of winter, caused by either an attack or service disruption of unknown origin, what should the government do? The traditional policy option is to manage the consequences of a service disruption. As part of the Federal Response Plan, first responders would provide blankets, temporary housing, medical care, and food. The federal government would then provide funding directly to the state governments to manage the impact of the power outage. Federal, state, and local governments use these political processes for natural disasters, and many in our government believe they are sufficient and appropriate for terrorist attacks as well.

An alternative approach would be for the federal government to provide direct benefits to the electricity providers to fix the problem—to restore service or to recover so as to mitigate the outage. Such benefits might include

As a policy matter, the government did not see how it could give aid to one company over another during the Y2K transition.

priority supply of goods or contracted services to fix the problem, loans, or loan guarantees. Of course, policies that mitigate and restore services provided by industry are dramatically different from those that feed, house, and cloth citizens.

As the Y2K rollover approached, federal leadership precluded approaches other than the traditional responses directed at the general populace. As a policy matter, the government did not see how it could give aid to one company over another during the Y2K transition. So honing in on the cause of the harm and mitigating that damage through assistance to an electric power provider for the nation's benefit was not a governmental policy priority.

This is a dialogue that must be revisited in the context of the current risk environment, and one that has dramatic implications for the insurance and reinsurance community.

The second area of risk covers responsibilities that are uniquely industry oriented. The private sector has a responsibility, made clearer from 9/11, to improve the security and reliability of critical infrastructure service delivery. Getting public companies to develop and enforce enterprise-wide risk management processes is an absolute industry responsibility. Federal and state governments can foster environments that promote risk management, but the duties, capabilities, and responsibilities remain in the private sector.

However, preliminary indications suggest that industry is not fully prepared to manage enterprise-wide risk in the aftermath of 9/11. According to a recent survey conducted by the National Association of Corporate Directors and Institute of Internal Auditors, corporate leaders are not sufficiently prioritizing risk management. According to the survey:

When asked, only 37 percent of directors responded that a formal enterprise-wide risk management process was in place in their organization, or that any other formal method of identifying risks was used. Even more alarming, 17 percent of directors surveyed stated that they did not know whether their company had a formal method for identifying risk.

Whether it is a matter of national security or simply good business practice, these statistics must change if the corporate community is to play its respective role in the evolving risk environment.

Beyond enterprise-wide risk management—and perhaps of even greater concern for the insurance and reinsurance community—is the question of how to raise the bar on security requirements and enhancements beyond the business case or concerns for ROI? Risk management in the current homeland security environment must be reexamined. Prior assumptions

Forrester Research concluded that by 2004, business-to-business e-commerce will approach $1.3 trillion. The Insurance Information Institute predicts that by 2006 this will translate into upwards of $2.5 billion in premiums to the insurance industry.

about threats, vulnerabilities, and critical business services must be part of a larger dialogue—one that occurs both within and across enterprises and sectors.

This is a daunting challenge, but one that the private sector must address. It is also a challenge that, once again, has dramatic implications for the reinsurance and insurance sectors, in terms of their ability to provide genuine risk transfer.

Finally, there is a third category of risks, those requiring immediate public-private cooperation. Here there needs to be far more discussion and exploration of the complex risk issues that involve shared threats and vulnerabilities across both public and private sectors.

An example following 9/11 underscores this point. The federal government manages the restoration of telecommunication services during a national crisis. During the World Trade Center recovery operations, and prior to the reopening of the financial markets, the federal government coordinated how telecommunications carriers and service providers restored telecom services. Well prior to the attack, public-private partnerships had already been grappling with the following issues:

What process should the government use to manage the restoration of telecommunication services?

More specifically, how should the government determine and assess where priority restoration should occur—especially where multiple telecommunications carriers and industries are affected?

How should the federal government prioritize two critical services in the same sector, such as clearing securities trades or payments issues?

Developing a restoration priority process requires a continuous dialogue within industry sectors, across different sectors, and with the government. It requires an honest and robust dialogue to guarantee that the restoration priorities chosen for national security or critical infrastructure purposes are followed. All critical infrastructure industries must participate in this dialogue so that restoration of service and recovery occur in a logical and prudent manner.

A second example involves development of a process for identifying and funding research and development that no single company can afford. Both public and private sectors will benefit from generating risk-related actuarial data and

modeling complex interdependencies. As this sector clearly understands, no single company should be required to generate, or be responsible for, all catastrophic risk modeling.

The federal government might play a useful role by helping to gather actuarial data for terrorism coverage, by participating in scenarios and war games, and by contributing to more sophisticated modeling of critical infrastructure harm.

The insurance and reinsurance industries are uniquely positioned to take a leadership role in pushing each of these dialogues forward.

CHAPTER 8

PANEL DISCUSSION:
Reinsurance and Terrorism

MODERATOR
Seán F. Mooney
Principal, Guy Carpenter & Company, Inc.

A few numbers provide perspective on the current situation of reinsurance and terrorism in the wake of 9/11.

The World Trade Center was a major facility: 24 million square feet, about 6 percent of Manhattan's total office space. It had 239 elevators.

When the complex was destroyed, the losses were enormous. They are currently estimated at $35 billion to $40 billion—twice the size of the prior record set by Hurricane Andrew in 1992.

About 60 percent to 70 percent of this loss is born by reinsurers. The price that reinsurers charged to cover this risk was almost zero. It was nearly nothing on the primary side as well, so it is not surprising that it is now difficult for reinsurers and primary companies to cover this risk at reasonable rates.

The surplus of the commercial lines insurance industry was $113 billion, as of the end of June 2001. It is even less now. This is quite a small amount to handle existing risks, plus all commercial insured terror risks in the United States. It needs to be supported by the reinsurance industry, which has significantly more capacity worldwide, approximately $280 billion.

The value of real estate at the largest commercial site in the United States, Manhattan, is $290 billion. Aggregate protection that could be compiled worldwide for terror risk—based on statements made in the market regarding existing carriers' stand-alone capacity—is about $20 billion, far below the $290 billion figure. The discrepancy between the need and the available capacity is enormous.

Bearing in mind this huge chasm between demand and supply, the following panel discussion explores the current reinsurance market to cover the terror risk. On the panel are four Guy Carpenter colleagues: Managing Director Kevin Stokes, Managing Director Charles Griffin, Principal Bill Plumb, and Senior Vice President John Major.

JANUARY 1 RENEWALS

Q: ***Sixty percent of reinsurance contracts in the United States are renewed on January 1. At the time of the most recent renewals on 1/1/02, what was the status of terror cover?***

Kevin Stokes: On property catastrophe business, clients with commercial portfolios found exclusions for terrorism essentially across the board. Reinsurers did provide coverage on personal lines risks, but excluded losses due to nuclear, chemical, and biological attacks.

On per risk business, reinsurers immediately after 9/11 excluded terrorism risk outright. However, as renewals progressed, the detailed information that was provided on accumulations allowed reinsurers to provide coverage on a restricted basis—for example, by way of a TIV exclusion clause. By this I mean that a specific dollar amount of the total insured value was instituted in the contract. For risks with liabilities below that value, there was coverage; above it, there was not.

Q: ***What was the situation at 1/1/02 for standard casualty reinsurance renewals?***

Charles Griffin: Early in the renewal process, reinsurers wanted to exclude terror cover on standard casualty protection. Insurers did not view their portfolios as having substantial terror exposure, and were upset.

As the renewal process evolved, reinsurers became more willing to discuss the specifics of a carrier's portfolio. During these discussions, new questions on casualty business arose. For example, geographic distribution of the book was an issue, a hitherto unusual concern for casualty. Reinsurers were also comparing the number of rural risks versus urban risks. They asked about "target risk" exclusions. Was terrorism excluded on the front end? If not, why?

When covers included workers compensation, reinsurers requested underwriting guidelines—particularly guidelines for managing aggregation of employees in any single location.

Reinsurers' comfort level with the answers to these questions, coupled with the experience of the treaty and the insurer-reinsurer relationship, influenced the degree of terror cover that was ultimately negotiated.

Reinsurers are a diverse group. Some were more liberal than others. And some cedent companies did not want to turn over their entire panel of reinsurers.

The situation also varied depending on whether it was a working layer cover, a casualty clash cover, or an umbrella facility. On working layer covers, when the premium-to-limit ratio was high and reinsurers were comfortable with the answers to terror underwriting questions, full coverage could be negotiated. As their comfort level declined, sublimits were introduced. If workers compensation was included, it was sublimited for full terrorism.

Recently, Guy Carpenter placed a cover for a book that had a large segment of churches. Despite the rural locations of these churches, reinsurers did not like this risk

from a terror point of view. The client could not exclude the terror risk on that business for competitive reasons, so reinsurers agreed to put an overall sublimit in the treaty. Ultimately, Guy Carpenter was able to negotiate some type of terror cover for almost all of our working layer business.

On casualty clash business, securing any terror protection at all on covers greater than $10 million proved difficult, especially when workers compensation was included, as it most often was. In these situations it made no difference how well a ceding company answered underwriting questions regarding terror risk.

Guy Carpenter was able to negotiate some terror protection on lower layer clash covers, if the program included a significant amount of personal lines business.

No market developed for stand-alone clash terror cover. In many placements, terror was provided outside of a target risk exclusion and sublimits for terror were provided when there was substantial premium in the program.

Q: ***What was the situation for workers compensation and professional liability?***

Bill Plumb: Workers compensation is a big issue since insurers are prevented by statute from excluding terror risk. The workers compensation reinsurance market has contracted, and there is limited terrorism protection available for workers compensation catastrophe risks. Similar to the protection granted on the property side, this cover typically excludes nuclear, chemical, and biological terrorism.

At January 1 workers compensation renewals, there was limited terrorism protection excess of the $100 million attachment point and under $10 million. The disconnect is in the $90 million excess of $10 million area. Part of the reason for this gap is that a greater number of reinsurers are required to fill out a placement in this area. Getting them all to agree to provide a certain amount of capacity is a difficult process.

At January 1, most but not all professional liability treaties were placed without a terrorism exclusion. Underwriting information was critical to the process. Reinsurers wanted to know how the insurance company was addressing the terror exposure on the front end.

Momentum is building to impose potential exclusions or restrictions on certain types of professional liability business, such as architects and engineers, insurance brokers, and medical malpractice.

In both workers compensation and professional liability, the situation is very fluid.

Q: ***What other trends, apart from terror cover being excluded, did you see in the marketplace at January 1?***

Bill Plumb: Information is critical. The way to address the disconnect that exists between the reinsurance and insurance communities in certain areas is to develop information that will enable reinsurers to analyze terror exposures.

As part of this effort, many cedents are now sending out applications asking for a per location headcount upon renewal of workers compensation. This was something no one was able to track previously simply because the question was not asked.

Reinsurers also want to know what the insurance company is doing to control underwriting exposure. How are they tracking aggregates, for example? These issues have become very important to reinsurers.

MODELING TERRORISM RISKS

Q: ***Will the extra data being collected assist in developing tools for underwriting and pricing terror risk?***

John Major: Detailed data on where employees are during the day will be important for terrorism modeling—not so much for developing models, but rather for putting the models to good use once they are available.

Modeling terrorism risk is complicated. The horrible number of lives lost on 9/11 made it clear that we have to look beyond property exposure. The first tools to come out from the modelers are for accumulation control. They are exposure-mapping tools, showing the location of concentrations of employees and property at risk. Using them effectively requires detailed data on employees and property.

But the real driving force connecting terrorism risk to workers compensation issues is the National Council on Compensation Insurance. The NCCI recently put out a request for a proposal to the modeling community seeking a terrorism risk model. This is important to the NCCI because while property writers can exclude terrorism risk, workers compensation writers cannot. The NCCI needs to be able to file rates in 34 states, so they need modeling assistance in a hurry.

Q: ***Where are the modelers in terms of analyzing terrorism risk?***

John Major: We can expect three waves of services and products coming from the modeling firms. The first wave is customized exposure mapping and scenario analysis with Geographic Information Systems (GIS).

The purpose of this is to highlight certain buildings or infrastructure features as potential targets, then see how exposures are distributed around them. Do you have numerous buildings in the shadow of the largest skyscraper in a central business district? If you do, you need to be concerned. The process is analogous to mapping earthquake fault lines and figuring the distance to insureds. It can be done today, but only as a customized service; it is not something carriers do on their own.

The second wave involves more formalized tools for accumulation control, building on GIS by automating "what-if" scenarios and making tools more user-friendly. For example, if a car bomb were set off at a certain location, what would be the consequences for a particular set of insured exposures? This can be done to some

extent today, but it is a customized and labor-intensive process. In a few months it should be more streamlined. A large part of the effort involves incorporating into the model the list of potential targets.

The third wave will be full-blown probabilistic models, which are much more sophisticated and similar to the models currently used with hurricanes and earthquakes. These will run through a large set of scenarios, with probabilities attached, and provide an entire risk curve with PMLs and return periods. It is tricky business, not only because terrorism is new ground for modelers, but because the risk is fundamentally different from any that has been modeled in the past. Expect to see disagreement between different models and significant changes from one version to the next as a model is updated. But such a model should be available by summer, if not sooner.

Q: ***What are the steps that modelers are going through to create terrorism risk models?***

John Major: The modelers must address four issues:

1. Where attacks might occur.
2. What form attacks might take.
3. What the probability is of a particular form of attack occurring at a particular location.
4. How to translate such an attack into damages.

Let's consider the *where* first. The major modelers all have databases of large buildings, bridges, tunnels, and other infrastructure. For example, AIR's "landmarks" database has some two million entries. Some interesting maps have been produced by Guy Carpenter's own cat modeling team showing locations of highway bridges, ports, oil facilities, and detailed information about office buildings and distance to possible targets. This sort of database is a natural starting point for defining targets and building scenarios around them.

However, since you cannot realistically focus on two million targets, the number needs to be narrowed down. One possible framework for this process is what Moody's Investor Services defined as three "tiers" of risk for commercial buildings. For example, there are 115 buildings in the United States that are more than 50 stories tall; 40 of these are in New York. These are in Moody's Tier 1. Other factors are noted as well. For instance, who is occupying the building—is it a well-known Fortune 50 company, especially in the media or defense sector, or a government agency? Public recognition is as important as sheer size, and proximity to highly trafficked transportation networks also matters.

Next, one must consider *how* an attack might occur. The biggest concern is a bomb, which is overwhelmingly the preferred mode of attack for terrorists. Next comes an airplane crash, then a chemical, biological, or even radiological weapon. Relevant attack modes are listed for each target. For example, if a building is surrounded by larger buildings, it is unlikely to be the target of an airplane attack.

The third step, after evaluating the *where* and *how*, is to assign probabilities to the combinations of targets and attack modes—

which is a very complex endeavor. RMS wrote a fascinating paper about the organizational structure of different terrorist groups and how that affects probability.

For example, the Palestine Liberation Organization (PLO) is more centralized and hierarchical than Hamas. The PLO can launch more sophisticated and potentially deadly attacks, but at the same time it is more vulnerable to counter-terrorist measures. You get this kind of insight only by hiring an expert or becoming an expert. Gordon Woo, the author of this paper, is an expert—not on terrorism, but on how to elicit probability judgments from experts. He is designing a questionnaire to do just that with regard to terrorism.

The fourth and last problem is how to translate a scenario into damages. For hurricane vulnerability, there is a significant amount of data from the field and from engineering studies illustrating how high winds damage buildings. For terrorism, the situation is comparable. There is a substantial amount of data and expertise on bomb blast damage and similar events. EQECAT, for instance, has a consulting group in San Antonio focused solely on blast effects. They also have a software program called MIDAS-AT (the "AT" stands for Anti-Terrorism), which models the dispersion of chemical, biological, or radiological elements in an indoor or outdoor environment. It has been around for 15 years, and has been licensed by the United States Marines.

Developing probabilistic terrorism models is an enormous undertaking, but the modelers are doing it.

Q: ***What about Guy Carpenter's work in this area—is there going to be a Guy Carpenter terrorism model?***

John Major: Guy Carpenter will be providing terrorism risk analysis, but not our own model per se. Our work currently focuses on clarifying the behind-the-scenes thinking that must go into developing a terrorism model. In addition, we intend to be expert users of the models that are created.

The type of question Guy Carpenter is working on is, for example, clarifying how the presence of human intent needs to be taken into account in a probabilistic analysis.

Consider a hurricane. The probability of a hurricane making landfall at a certain location has nothing to do with the value of the buildings there, nothing to do with the existence of a protective seawall, or anything else about the human environment. Nature, for the most part, does not care what humans do. A terrorist does.

A terrorist cares very much about the value of targets and how they are defended, so you need to go beyond the mathematics of probability and think in terms of Game Theory, which was popularized by the movie "A Beautiful Mind."

Essentially, the conclusion is this: The more attractive the target, the less likely it is to be successfully attacked. This runs counter to what one might intuitively expect, primarily for two reasons: First, the way in which defenses are allocated; and second, how the attacker adapts his behavior to those defenses. It is not the sort of thing you need to consider with hurricanes and earthquakes.

STAND-ALONE TERRORISM COVER

Q: ***What is the status of stand-alone reinsurance cover for terrorism risks?***

Kevin Stokes: At January 1, a number of stand-alone property catastrophe programs covering losses only from terrorism were put in place on behalf of our clients, including both national and regional companies. Naturally, this cover dovetails with the main property program, so while it is terrorism coverage it still excludes nuclear, chemical, and biological attacks.

Q: ***Would you also expect to see some facultative cover behind that?***

Kevin Stokes: Absolutely. The ceding company is using facultative to manage that risk as well. It is actually a better fit for risk-by-risk underwriting.

POLICY WORDING

Q: ***Is any consensus emerging in terms of wording for a property terrorism exclusion?***

Kevin Stokes: Definitely. On the catastrophe side, NMA 2930 Versions A and B are emerging as a standard. The basic difference between A and B is that B has a write back for personal lines coverages.

However, Guy Carpenter believes that there are a number of areas where this wording can be improved. For example, the definition of terrorism on original business should be amended to clarify that events that were covered prior to 9/11—such as riots, vandalism, and malicious mischief—are still covered and not swept up in the definition of terrorism.

In the United States, there needs to be a governmental authority designated as the arbiter of what is and is not a terrorism event. A few months ago a youth in Tampa, Florida, flew a plane into a building. The insured loss in this case was not large, but the situation illustrates how a dispute could arise with reinsurers as to whether the act is terrorism or not. In this particular case, the government stated that it was not a terrorism event.

The exclusion should also be for direct losses. Language referring to "indirectly" should be eliminated.

Q: ***Any agreement on terrorism exclusion language on the casualty and specialty side?***

Charles Griffin: There is no move right now towards one specific exclusion wording. Individual reinsurers have definite opinions that their particular wording is the correct wording, and negotiation continues.

A key issue being considered on workers compensation catastrophe cover is the definition of "event." The workers compensation catastrophe product was originally developed for events such as an earthquake, which in theory is specific to time and place. In the realm of terrorism, that wording may not work. Even in the case of the World Trade Center, arguments can be made, given specific time and

place wording, that the attack consisted of two separate events.

Generally, the industry agreed for property and casualty reinsurance purposes that it was one event. But these are the types of things that still need to be considered on casualty contracts.

Q: ***Would reinsurers prefer language viewing the Pentagon and the World Trade Center as separate events?***

Kevin Stokes: I believe reinsurers would prefer not to aggregate them. On the other hand, our clients would prefer, as a general rule, that the Pentagon and the World Trade Center be considered one event since the attacks had a common origin, so losses would be aggregated.

Q: ***What seems to be the perspective of most insurers regarding "hours clauses," which set the time period within which losses can occur and be considered a single event?***

Charles Griffin: Most Guy Carpenter clients are willing to accept some type of hours clause—most often in the range of 168 hours for workers compensation.

Q: ***The "fire following" issue is a particular problem for insurers writing in certain states, such as New York. What can be done to help companies with that type of exposure?***

Kevin Stokes: Fire following on catastrophe business would be excluded by the emerging standard NMA-2930, both versions. Fire following would be available under stand-alone coverage.

To address this issue, some ceding companies are moving business from an admitted to a non-admitted status. They are also amending underwriting in terms of accumulations at any one location and the surrounding area, and arranging facultative reinsurance to address the fire following issue as well.

Q: ***The Accident & Health carve-out market for workers compensation catastrophe cover essentially collapsed after 9/11. How has the reinsurance market addressed this loss of capacity?***

Bill Plumb: The workers compensation catastrophe market is expanding, although it is not where it was before September 11, when it was dominated by the A&H market.

The A&H market has dropped from about $600 million to $50 million aggregate capacity. Many A&H markets have been pulling out, but P&C reinsurers are coming into the business.

I estimate the total workers compensation catastrophe capacity available from the P&C side today at approximately $300 million. However, that number is a bit deceiving, since some of those markets play in the exact same areas, creating overlap. It is probably more likely that approximately $200 million to $250 million of workers compensation catastrophe protection could be put together today.

THE FUTURE

Q: ***Looking ahead to upcoming renewals, what should we expect in terms of terror cover?***

Charles Griffin: I do not expect that terrorism cover is going to be any easier to secure within existing treaties between now and yearend. Reinsurers' retrospective programs do not include it; reinsurers are writing net lines for it. However, stand-alone cover should be attainable next to risk programs and hopefully clash programs as well, as models are developed and reinsurers become more comfortable with the risk.

Bill Plumb: I agree that the situation will not change dramatically by yearend, although progress will continue to be made. Two weeks after 9/11 the industry said that terrorism would be excluded, period. We have come a long way from that point. Terrorism protection is available. Insurers and reinsurers will become more comfortable with the exposures. It is similar in some ways to what happened after Hurricane Andrew, when the reinsurance community suddenly said it needed data to analyze the exposures. Only now the data is different. It is more specific to locations and to headcount. Insurance companies are trying to develop this information, which will give reinsurers the ability to evaluate the exposures going forward, and the market will settle down.

Kevin Stokes: Midyear renewals should reveal whether the NMA 2930 is truly the standard wording and whether or not any of Guy Carpenter's suggested amendments will be incorporated into the wording.

On the per risk side, we will continue to see coverage provided on a case-by-case basis, or perhaps sublimited. However, we do expect outright exclusion to continue on national large account business.

CHAPTER 9

Reinsurance Solutions to the Terrorism Issue

Britt Newhouse
Managing Director,
Guy Carpenter & Company, Inc. and Marsh

Christopher B. Royse
Principal, Guy Carpenter & Company, Inc.

Since 9/11 it has been hard at times for brokers to remain optimistic. But that is just what our clients and markets want and expect from us.

The common refrain heard at industry conferences around the world is that the reinsurance and insurance industries "really missed it" on the three largest systemic causes of loss that have occurred in our recent history: asbestos, pollution, and now terrorism.

The industry did not intend to provide coverage, nor did it price for the catastrophic social costs these perils inflicted. The industry points woefully to the impact on results and the casualties on the sidelines as evidence of its failure to limit itself to providing coverage only for what it knows.

Some say all risk coverage must end once and for all. This argument usually comes from the underwriters who have paid enormous claims, not the brokers who are collecting claims for clients who are now realizing the value of insurance for the first time in many years.

As a broker—and therefore an optimist—I disagree. Notwithstanding the fact that the industry did not recognize and price for these risks before they became evident, or that society to a large extent decided how the industry would respond after major losses occurred, the insurance and reinsurance industries have performed incredibly well on the whole, with relatively few casualties in relation to the scope of these risks and their impact on society.

A large part of the asbestos, pollution, and now terrorism risk was absorbed by our industry and spread over the economy and over time.

Granted, there were many serious casualties: dismal results, insolvencies, and departing CEOs, CFOs, and CUOs. But this is not like the S&L industry in the 1980s, Japanese banks in the 1990s, or the steel and airline industries in the 1960s or the 1990s.

For the most part, our system has worked and is working to cope with these social strains. Our industry continues to act as the oil that keeps the social machine running relatively smoothly.

THE "UNMANAGEABLE" TERROR RISK

What does the current "unmeasurable, unmanageable" risk of terrorist attack have in common with asbestos and pollution exposures?

Accumulations are enormous and were largely unforeseen.

Coverage is being applied as broadly as judges can apply it.

There is tremendous social and political pressure to respond and to continue responding to the risk.

The big difference is that pollution and asbestos were not the results of a coordinated human effort to cause the maximum amount of human suffering and property damage in the shortest possible timeframe.

Pollution and asbestos were caused by human activity, but they did not spontaneously combust, and they were not consciously intended to produce the results that they ultimately did.

THE HUMAN BEHAVIOR FACTOR

The most frightening thing about terrorism risk is that it is driven by human behavior. Human behavior is hard to measure, predict, and manage. It is especially difficult to manage if the driving proximate causes are social, political, economic, and religious pressures that cross borders and continents. They would appear to be forces that we cannot influence.

This is not the first time our industry has dealt with the human behavior peril. Once before, we experienced unforeseen accumulations of property and bodily injury exposure arising out of the human behavior peril, also caused by social, political, economic, and religious pressures that crossed boundaries. It was the riots and civil commotion of the 1960s.

The insurance and reinsurance industries excluded this peril in the 1960s and 1970s as being unmeasurable and unmanageable. Now, for the most part, it is once again treated as an insurable peril. This is to some extent because society evolved to alleviate some of those pressures. Society made progress on the social, economic, political, and religious pressures that were causing the behavior—enough progress, at least, to change the way humans reacted to these pressures.

The problem we now face is one that we as a society have a better chance of managing and influencing. We must find those individuals responsible and morally engage in risk management and risk intervention. This can be done at the same time that steps are taken to help alleviate the underlying social, economic, political, and religious causes.

While this happens, the free market economy is going to stimulate our industry to find ways to manage the risk.

EVOLVING INDUSTRY SOLUTIONS

The industry has always responded by seeking a way to manage the risk. Piece by piece, brokers will start segregating the risk, repackaging it, and spreading it around.

Piece by piece, brokers will start segregating the risk, repackaging it, and spreading it around.

The federal government may step in, or it may not. It may wait and see how the industry manages, then offer a remote backstop to ensure confidence, much in the same way that the FDIC prevents runs on the banking industry.

Both insurance and reinsurance products are already evolving. These have and will include combinations of the coverage, pricing, pooling, and post-loss financing that our industry has applied in the past.

The formula includes starting with a group of exposures that are understandable, homogenous, and offer some spread of risk and diversification. The mechanism must be simple and clearly understood by all that buy and sell it. Over time, the coverage will broaden, and the risk-spreading mechanism will apply to more and more risks exposed to this peril.

In the next section of this report, Chris Royce describes such an approach.

REGIONAL INSURER POOL FOR TERRORIST ATTACKS

Regional carriers are concerned about terrorism exposures, but their needs are different from those of carriers who were heavily impacted by 9/11. Like all companies, they are concerned about the gap between their policies and available reinsurance coverage, and the potential for losses from future terrorist attacks, particularly in the absence of a government facility. Regional carriers, however, have more discretion than national carriers in regard to stand-alone cover, since regional carriers do not typically write target risks. They typically have smaller limit requirements than the national stock carriers, and they are more price-sensitive in terms of how much they are willing to budget for this protection.

Guy Carpenter is involved in the development of a regional insurer pool for terrorist attacks. For the pool's target membership—essentially insurers with Main Street commercial and personal lines business—regulators are allowing limited terrorism exclusions on filed form commercial risks in most states. Filed forms in New York, California, and Illinois prohibit terrorism exclusions. In 28 states, fire following loss is covered even when the terrorism exclusion is allowed. In addition, a $25 million industry loss is required to trigger the terrorism exclusion.

THE CONCEPT

Part of Guy Carpenter's hypothesis in developing this facility is that regional carriers can reduce terrorism exposure, but they cannot eliminate it entirely. With the right terms and conditions, a segment of this regional market will purchase stand-alone terrorism coverage. The intention of the pool is to give regional companies access to this

coverage with attractive terms and conditions.

The concept of the pool is based on the following premises:

- The absence of significant open market pricing in agreed-upon rating mechanisms. A pooling arrangement makes sense when the rating of the product is uncertain; if the premium is too high, there is a mechanism for recapturing some of the premium.
- A pooling arrangement among insurers can effectively spread the risk and minimize the cost of coverage.
- The collective purchase of reinsurance by the pool most efficiently accesses additional capacity.

COVERAGE OUTLINE

The coverage provided by the pool is designed to align with property catastrophe product concepts. Losses-occurring coverage is provided on an annual term, with all members' programs incepting at a common anniversary date. May, 2002, is the coverage inception.

The cover is intended to fill the gaps created by terrorism exclusions in traditional property catastrophe products. The product would provide a limit of $10 million per occurrence and in the aggregate per member. Guy Carpenter expects that this limit will adequately address the needs and budgets of prospective pool members. At the same time, the limit does not provide any carrier with a competitive advantage; it addresses an otherwise unprotected exposure.

Coverage includes losses resulting from nuclear, chemical, or biological attacks, which are typically excluded across the board on property catastrophe reinsurance contracts.

The retention for each individual member would be equal to their current property catastrophe retention or $2 million, whichever is greater. Similar to a traditional property catastrophe program, coparticipation would be 5 percent.

This product is not intended to create capacity for members to write risk or perils that they otherwise would not. There are specific exclusions associated with the product, such as:

- policies specifically covering terrorism
- coverage for risks in the utilities, telecommunications, and aviation sectors
- target risks, e.g., the Empire State Building
- contingent business interruption.

Exposures such as utilities and target risks are not large components of the portfolios of the vast majority of prospective pool members, so they should be relatively easy exclusions to accept.

Losses triggered by natural perils that would be covered under a standard property catastrophe program would also be excluded, and coverage would have standard property catastrophe conditions, such as a third-party liability exclusion, a war risk exclusion, and the requirement of a two risk warranty with to-be-agreed-upon per risk limitations.

CLAIMS-PAYING ABILITY

In its initial year, the pool aims to attract 50 members. Annual aggregate claims-paying ability would be the sum of the net reinsurance premium, plus the reinsurance commitment, plus investment income, less management fees.

The pool itself would retain and pay for the first $10 million of claims to the facility; it would then rely on a reinsurance contract generating $90 million excess of the first $10 million of loss. This creates claims-paying capacity of $100 million.

The pool would be subject to an occurrence cap of $40 million, which is intended to ensure the pool's ability to withstand multiple events and provide protection to pool members against a single geographic zone exhausting claims-paying capacity. A spread of geographic risk is important as well.

All insurance and reinsurance contracts are subject to the aggregate claims-paying ability of the risk bearer, this pool is simply more explicit regarding that limit.

Pro-ration of recoveries would occur if aggregate losses exceed the $100 million claims-paying ability.

PRICING

The goal in pricing this cover is to minimize the cost of the product to the members, while generating enough aggregate premium for the pool to internally fund losses and enhance claims-paying capacity with reinsurance.

Currently, the target is a flat price of $500,000 per member, which is slightly more than 5 percent rate on line for 95 percent of the $10 million limit. The plan is that $475,000 of that would go toward the reinsurance premium, with a $25,000 administrative fee covering the expenses of the issuing facility. Because it is a pool, the membership would be subject to retrospective premium assessments up to an additional 2 ½ percent rate on line. That is potentially an additional $250,000 per member, if the pool has losses. These assessments would occur when $10 million to $35 million in aggregate claims are ceded to the pool.

While the retro feature is not expected to be well received by members, it is likely to occur during a period when new capacity for terrorism coverage is even more precious than it is now—that is, after several more events have occurred.

REINSURANCE LOGISTICS

A Special Purpose Vehicle (SPV) would be used to create a cell dedicated to this pool. This SPV would purchase reinsurance on behalf of pool members, issue reinsurance contracts to members, and handle assessments of retrospective premiums.

Membership in the cell and the pool includes voting rights. Since all members would contribute equal premiums in the first year, all original members would have equal voting rights. An officer and a board of governors would be elected by pool members for ongoing management of the facility,

With the current lack of a federal terrorism solution, the pool can provide coverage for the next few events.

and the mission of the facility going forward would be determined by the members and the duly elected management. They would decide such issues as dividend payments in the event of profitable experience, coverage amendments, pricing issues, and the pool's expansion to other members and other products.

With the current lack of a federal terrorism solution, the pool can provide coverage for the next few events. Should future events prompt the government to create a facility, the pool may continue to be attractive since it would provide coverage for that portion of a loss that the industry is required to retain before federal intervention.

Before rolling out this concept to potential pool members, there needed to be a sense of the viability of the reinsurance structure. Five reinsurers selected have all responded quickly with a qualified endorsement of this facility. These five carriers are ACE Tempest Re, Axis, Converium, Transatlantic Re, and XL Mid Ocean Re.

WHAT'S NEXT

Discussion of this concept with Guy Carpenter brokers nationwide has begun. A list of potential pool members has been submitted. This first round of submissions identified 55 regional companies as potential pool members. The list also generated the geographic exposure that is needed for this facility.

This pool approach focuses on a specific segment of the insurance marketplace, attempting to capitalize on its inherent spread of risk and the homogenous nature of its exposures. It is not the answer for all carriers, but, if successful, the approach can be applied in the future to generate capacity for clients in other industry segments.

Next Steps

Gregory T. Doyle
Executive Vice President,
Guy Carpenter & Company, Inc.

We have heard from the experts. The terror risk is here to stay; and it must be mitigated. Our industry cannot meet this challenge on its own, nor can the federal government.

Success in managing the terror risk will come only through unprecedented collaboration between the public and private sectors. The insurance and reinsurance industries must play a pivotal role—a leading role—because the tools and techniques to assess, quantify, and manage the risk are within our grasp.

So what do we do now? We need to move forward in at least four key areas:

1. We must find a way to assess the terror risk. As part of this effort, we will be working with our government, which has collected information and data on the risk of terrorism over the years.
2. We must understand and model the terror risk. The modeling firms are starting to address these issues. Guy Carpenter and others need to put forth ideas to refine the approaches currently being undertaken.
3. We need to define coverage more clearly, and with much more uniformity. Contract wordings have been difficult, because definitions of the terror risk are based on the understanding of the exposure, which has been limited thus far. As our understanding of the risk improves, we must continue to move closer to agreed-upon language.
4. Lastly, we need to better define risk mitigation strategies. Again, with our government's help, we must employ ways to protect ourselves against this risk—as a country, and as an industry. Heightened security will be an ongoing part of the solution, and more can be done once we understand the nature of the risk.

Can the terror risk be managed? Indeed, it can.

We have engaged the experts, and framed the issues. We are focusing on solutions. And now, we are all better equipped to make such solutions happen.