The Critical Infrastructure Protection Program July 2005 / Volume 4, No. 1

THE CIP REPORT

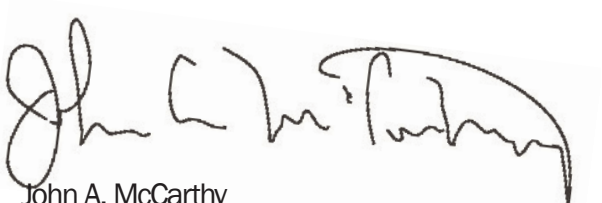
Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here. Visit us online for this and other issues at http://cipp.gmu.edu

Insuring critical infrastructure has long been a topic of great intensity and controversy, due to the potential for devastating losses as well as the complexities inherent in the cyber aspects of critical infrastructure. The consequences of potential catastrophic events and their resulting financial damages require continued efforts to explore mechanisms that would increase the insurance industry's capacity to respond. One such effort underway here at the CIP Program resulted in a recent workshop on "Protecting the Electricity Sector's Infrastructure: Building the Business Case for Commercial Insurance." This workshop, sponsored by the Department of Energy and the National Energy Technology Laboratory, is highlighted in this issue of *The CIP Report* and provides an example of one sector's efforts at increasing resiliency through the use of commercial insurance.

Also included in this month's issue are contributions from Dr. Kenneth Freidman of the Department of Energy's Office of Electricity and Energy Assurance, Christopher Keegan of Marsh, Inc., and Dr. James Atkins of Regulatory Heuristics, all of whom work on various aspects of insuring infrastructure. Their contributions, in addition to supporting articles on the debate over terrorism risk insurance (TRIA), the GAO's report on Catastrophic Risk, and research out of the George Mason University School of Law, provide insight into the ongoing discussion regarding the role insurance should play in critical infrastructure protection.

In addition to these articles, we are pleased to feature articles detailing James Madison University's recent release of their second annual Citizen's Guide, "Protecting Ourselves: A Rural Guide for Emergency Preparedness." Finally, we provide a brief overview of the Privacy Conference held by former Secretary of the Army and Senior CIP Program Scholar John O. Marsh, Professor Angeline Chen and the CIP Program on June 16, 2005. This event brought together distinguished thought leaders within the Privacy community and sparked valuable discussion informing this vital policy area. Conference recommendations are currently being compiled and will be released shortly.



John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University, School of Law

Terrorism Risk Insurance Act Up for Renewal

Colleen E. Hardy, J.D.
CIP Program Senior Legal Research Associate

In the aftermath of the September 11, 2001 attacks, insurance companies took the brunt of the economic devastation. Insurance companies paid billions of dollars to businesses and individuals without any government assistance. It was estimated that insured losses resulting from the September 11th terrorist attacks were nearly $32.5 billion. These losses caused insurance companies to rethink insurance coverage for terrorist acts. At that point, the government stepped in with an interim three year plan called the Terrorism Risk Insurance Act (TRIA). TRIA is set to expire in December 2005, unless renewed by Congress. The government and the private sector are debating whether TRIA is still needed.

What is TRIA?

Emily Frye, Principal Consultant for Critical Infrastructure Protection, Touchstone-SRA, Inc., has been studying the relationship between catastrophes and insurance, and she summarizes TRIA this way: TRIA requires that insurance companies make terrorism risk coverage available to all customers, and in return, guarantees that the government will provide federal reinsurance (a "backstop") for any losses above a certain amount. TRIA also requires that the government cover 90% of terrorism-related losses (up to a total of $100 billion) once insured losses reach certain levels. TRIA covers certain lines of commercial insurance, the most prominent being commercial property, business interruption, workers' compensation, and general liability.

What is the debate?

Supporters of extending TRIA claim that without TRIA's financial backstop in place, the federal government could be left solely responsible for funding both the direct costs of catastrophic terrorist attacks, as well as the longer-term costs associated with economic recovery in the wake of such attacks. However, those who oppose the extension of TRIA question how the insurance companies will establish their own reinsurance market for terrorism if the government provides the service for free.

What has research concluded about TRIA?

In a recent study conducted by the RAND Corporation, researchers determined that the terrorism insurance system is not strong enough to respond to a rapidly evolving terrorist threat against US businesses. The RAND study concluded that Congress should improve the financial protections offered by TRIA by expanding TRIA to cover chemical, biological, radiological, and nuclear (CBRN) attacks, and attacks by domestic groups.

Several other individuals have urged that any extension of TRIA should include CBRN and domestic attacks. The CIP Program recently hosted a Department of Energy workshop on protecting the electricity sector's infrastructure. Many attendees, in both the insurance business and energy sector, argued that it is imperative to include CBRN and domestic attacks if TRIA is going to be extended. Ms. Frye stated that the absence of protection for CBRN and domestic attacks are significant gaps in TRIA.

Colleen Hardy

The United States Department of Treasury has also conducted research on TRIA. This study concluded that TRIA has been effective in achieving its temporary objectives and has provided a transitional period during which insurers enjoyed enhanced financial capacity to write terrorism risk insurance coverage. However, the Treasury Department also determined that the sunset of TRIA would encourage the development of the private reinsurance market and other risk-transfer mechanisms. They recommend extending TRIA only if it (1) includes a significant increase (to $500 million) of the event size that triggers coverage; (2) increases the dollar deductibles and percentage copayments; and (3) eliminates from the *(Continued, Page 12)*

Building the Business Case for Commercial Insurance in the Electricity Sector

Dr. James B. Atkins
Regulatory Heuristics, LLC

On June 22-23, 2005, the Critical Infrastructure Protection Program (CIPP) at George Mason University School of Law conducted a workshop on "Protecting the Electricity Sector's Infrastructure: Building the Business Case for Commercial Insurance." A diverse group of 35 national and international experts from the electricity and insurance sectors discussed and debated the current role of insurance in the electricity sector and the potential for insurance to promote future electricity sector infrastructure protection. The U.S. Department of Energy (DOE) and the National Energy Technology Laboratory (NETL) sponsored workshop included participants from various federal agencies, the U.S. Congress, the Organisation for Economic Co-operation and Development (OECD), academia, insurance companies, engineering consulting firms, public and investor-owned utilities, the Edison Electric Institute, the North American Electric Reliability Council and energy sector publishing.

The workshop opened with John McCarthy, Director of the CIPP, providing a brief introduction to the project. He welcomed the opportunity to work with the workshop participants and the DOE on this important work. Kevin Kolevar, Director of the DOE's newly established Office of Electricity and Energy Assurance (OE), stated that the OE is focusing on identifying electric system vulnerabilities, system protection, restoration and disaster recovery. He referenced the catastrophic 2004 hurricane season in Florida and the Southeast as an example of the need to focus on disaster recovery. He stated that this workshop "should provide a dialogue for developing recommendations to develop policy and a business case to create greater electric system resiliency." Dr. Ken Friedman of DOE stated that OE is currently looking at various tools for finding solutions to issues in the electric sector. He went on to note the importance of this collaborative workshop was to "build a business case for commercial insurance whether for natural hazards or terrorist threats, especially threats of low probability and high risk."

...the establishment of mandatory, enforceable reliability standards was a critical component to not only improve reliability in the electricity sector, but also to better define insurance risk through improved data reporting and compliance monitoring...

Participation by the insurance industry with DOE and the electric sector is "necessary to clarify the linkages between insurance and the electric sector in order to build a business case."

A main discussion point during the facilitated workshop was that few, if any, insurance products exist for transmission or distribution (T&D) systems. T&D assets are typically "self insured" through some form of reserve or capital fund maintained by the respective energy companies. Due to the current regulatory status of the electric sector, cost recovery by transmission-owning companies through such self-insured funds is generally subject to State Public Utility Commission approval. In the case of the 2004 Florida hurricanes, repair costs to the electricity system far exceeded the value of these reserve funds. A range of possible cost recovery alternatives were discussed such as requiring mandatory insurance for all transmission systems, or using various insurance instruments as a supplement to self insured reserve funds. However, "adverse selection," the phenomenon where the only parties interested in the insurance are those that need coverage the most, remains a major obstacle to insuring such infrastructure impacts.

A consensus was reached among the *(Continued, Page 10)*

Energy Utilities and Catastrophe: Examining Insurance as a Means of Cost Recovery

Dr. Kenneth Friedman
U.S. Department of Energy

The U.S. Department of Energy (DOE) and the National Energy Technology Laboratory (NETL) are supporting work at the CIP Program to examine the role insurance could play to support or encourage critical infrastructure protection in the energy sector. The new post 9/11 challenges to the U.S. energy infrastructure from both physical and cyber threats is the basis for the current GMU effort. This work seeks to engage both the utility and the insurance industries, as well as the regulatory agencies, in a dialogue on how insurance could be used to manage or reduce physical/cyber and financial risks to energy assets and how insurance could be used to help speed recovery from catastrophes.

The Florida hurricanes of 2004 demonstrated the potential of insurance to mitigate the financial consequences of major natural and man-made events. Stricter underwriting standards imposed by the insurance industry after Hurricane Andrew in 1992 may have limited somewhat the damage from the 2004 storms. The four hurricanes that struck Florida caused over $20 billion in overall insured damage. Utility storm reserve and rainy day funds, generally maintained by utilities as a form of "self-insurance," were exhausted by the historic magnitude of the recovery efforts. Starting August 13, 2004, four hurricanes hit Florida in less than two months-Charley, Frances, Jeanne and Ivan. The scale of the impacts on Florida utilities can be represented by the three storms that went through Florida Power and Light (FPL) territory which hit power plants, downed power poles and electric wires, and disrupted electric service to 5.4 million customers, according to the company. The company and its employees were in a "hurricane restoration mode" for almost six weeks. Using their own employees, other utility workers and contractors from 39 states and Canada in a restoration workforce ranging from 13,000 to nearly 17,000 people, the company was able to restore power increasingly quickly, learning from each storm that passed through. More than 13,000 power poles, 11,000 transformers and 1,700 miles of conductor were replaced to restore the electric system.

The cost to FPL of this enormous effort was $545 million and the combined costs to FPL and Progress Energy were over $1 billion. The $1 billion in costs, plus the additional costs to Gulf Power and Tampa Electric were borne by the utilities. Special storm reserves set aside by FPL served as a form of self-insurance, and covered $345 million of the $545 million in recovery costs. A February 2005 report by the Edison Electric Institute, "After the Disaster: Utility Restoration Cost Recovery," addresses the various tools the electric utilities use to lessen financial impacts of disaster restoration. The study, which was based on data obtained for 81 major storms and from 14 utilities between 1994 and 2004, found that utilities expended approximately $2.7 billion to recover (*Continued, Page 12*)

> *"What is ironic, given the importance of storm restoration, is that more established and consistent policies regarding storm recovery are not in place. From a cost recovery standpoint, why is recovery of storm restoration costs any different from recovery of insurance premiums? Both represent a cost item for operating a modern utility. Yet, the industry has vastly different philosophies regarding cost recovery of these two items."*
>
> From *After the Disaster: Utility Restoration Cost Recovery*, Edison Electric Institute

Information Risk: Meeting New Threats and Challenges

Christopher Keegan
Marsh, Inc.

Every minute of every day, thieves, extortionists, vandals, and other hackers probe the Internet for security holes in your organization's computer networks. Some of the threats to your business come from organized criminals operating outside the United States. Other perpetrators reside much closer to home–it is estimated that 75 percent of attacks originate from employees, contractors, service workers, and other insiders. In the rapidly changing world of information technology (IT) management, one thing is virtually certain: Your computer network will be attacked. In fact, one in four companies can expect to experience a significant Internet security incident by the end of 2005, according to the research firm Gartner Group.

The information on your organization's computer network is one of your most valuable assets, meaning threats to it are a critical risk. Meeting your information security needs requires a framework in which the appropriate people, processes, and technology are backed up by strong policies and standards. Such a foundation provides the catalyst to integrate information security and information technology continuity into your risk management strategy; helps set priorities for security investments; and builds confidence with customers, employees, business partners, and regulators.

Information Risk

Information risk refers to a component of operational risk that a company faces because it relies on the integrity, confidentiality, and availability of electronic data and technology systems. The more damage a business can suffer due to the unauthorized modification, disclosure, or destruction of its data and information technology, the higher its information risk and the greater its information security needs. In other words, a mom-and-pop business that only uses a personal computer to pay bills online carries much less risk than an international financial services firm that has significant online operations, transfers vast amounts of information over the Internet, employs thousands of workers with access to its system, and keeps confidential files on millions of clients, customers, and partners. One way to look at information risk–and most other risks–is to see it as the product of three factors: threat, vulnerability, and asset value.

Information Risk = Threat x Vulnerability x Asset Value

Threat is the probability that something bad will happen to information assets through such causes as accidental or deliberate physical damage, equipment malfunction, human error, attacks on your network, misuse of data, and loss of data.

Vulnerability is the strength of your controls, including the technologies, human practices, and policies you employ.

Asset value is the tangible or intangible value of the information resources you wish to protect. It includes such items as knowledge about clients, intellectual capital, vendor and supply-chain information, and so forth. With information risk, asset value also includes the potential for liability.

Who Is At Risk?

Nearly everyone is affected by the security of information, from consumers who depend on their personal data being kept confidential to corporate officers who potentially face lawsuits if security is breached:

- Consumers face a number of risks. If an individual's confidential information--name, address, account numbers, passwords, and so on--is stolen, he or she may fall prey to

Information Risk = Threat x Vulnerability x Asset Value

(Continued, Page 6)

Information Risk *(Cont.from Page 5)* identity thieves. Victims of identity theft spend an average of $1,400 and 600 hours of their time clearing their names and credit histories after such a breach.

- If a client company's confidential information is stolen, it may be at risk not only for a form of identity theft, but also for extortion. Clients may also face problems with their supply chains if a cyber attack forces your company to suspend operations. Loss of critical information can result in a loss of competitive advantage.

- Directors and officers face an increased threat of lawsuits related to information risk. For example, the Sarbanes-Oxley Act of 2002 (SOX) holds directors and officers responsible for the effectiveness of their companies' internal controls. The nature of modern business is such that it would be nearly impossible for a company not to have a significant IT component to its internal controls. A failure in internal controls could lead to a securities class-action lawsuit naming directors and officers.

- Corporations and their shareholders face a number of risks when information is threatened or compromised. Businesses may have to shut down critical systems, losing revenue. They may face costly litigation if sued for third-party liabilities such as intellectual property infringement, content and advertising-related offenses, invasion of privacy, loss of data, and errors and omissions.

- In a larger sense, the viability of e-commerce is at risk. As consumers hear more horror stories about identity theft, they may become less likely to conduct transactions online. And as businesses–particularly small to mid-size firms–are named in lawsuits related to information risks, they may be less inclined to include e-commerce in their business models.

Managing Information Risk

Instead of only analyzing how a cyber attack would affect individual business units, such as the IT department or the billing department, companies must consider how a security breach would affect the entire enterprise. In other words, managing IT risk must be integrated with the overall risk management strategy. Technology infrastructure-servers, network monitors, firewalls, and so on-needs to be assessed and managed in terms of its relation to people, operations, supply chains, and other business drivers. Some of the steps involved with IT risk management include paying attention to human factors, putting proper security policies in place, identifying critical assets, and fostering better communication and an enterprise-wide perspective among IT managers and risk managers.

Insurance Solutions

The insurance industry's response to the increasingly networked nature of business has been fairly predictable. Caught off guard in the 1990s by claims related to loss of data-which had not been anticipated in most traditional policies--insurers rewrote policy language to exclude cyber and network risks from traditional property and liability policies. At the same time, insurers recognized that clients would demand something to replace those exclusions, leading to the development of e-business insurance, also called cyber or network risk insurance.

Christopher Keegan
Marsh, Inc.

Cyberexclusions in Traditional Policies

In 1999, a major ISP released a new version of its access software. Soon after, users filed more than 40 lawsuits claiming that installing the software caused important data to be lost. The company settled the lawsuits for a total of about $15 million and filed a claim with its insurer to try to recoup under its commercial general liability (CGL) policy. The insurer rejected the claim, and the case wound up in court. In 2003, the 4th U.S. Circuit Court of Appeals upheld a lower court ruling in favor of the insurer. The courts agreed with the insurer that loss of data did not qualify as "physical damage" to "tangible property."

The ruling and others like it have a significant impact because both CGL *(Continued, Page 11)*

A Summary of Michelle Boardman's

"Known Unknowns: The Delusion of Terrorism Insurance"

Tim Goobic, CIP Program Intern
University of Kentucky

George Mason University Law Professor Michelle Boardman published a paper on terrorism insurance this past March focused on a thorough examination of a current federal requirement which forces all insurance companies to provide terrorism coverage. "Known Unknowns: The Delusion of Terrorism Insurance" is divided into six sections which examine the topic of mandated terrorism coverage. Professor Boardman concludes that it is incalculable and prohibitively expensive to provide and that the reality of this situation needs to be more clearly communicated to the American people.

Prior to September 11th 2001, insurance companies did not specify potential "terrorism" losses as the risk was considered very low. However, following the events of 9/11, the risk of terrorism has been considered too high, too volatile, and too uncertain to be priced. While this prompted many insurance companies to exclude offering terrorism coverage, Congress intervened and enacted the Terrorism Risk Insurance Act (TRIA). The TRIA program barred insurance companies from excluding terrorism coverage in exchange for federal funding in catastrophic loss scenarios. Boardman's piece contends that in reality, terrorism risk cannot be covered now or in the future because of the sheer uncertainty of terrorist events. Terrorism risk can include everything from relatively minor explosive damages to wide-scale destruction.

Boardman asserts that risk cannot be calculated because there is not enough actuarial data to calculate the likelihood, nature, or extent of the risk. If an attack is catastrophic, such as a nuclear bomb, it cannot be insured because such great loss compromises the value of risk pooling across geography and policyholder type. TRIA is set up with insurers paying everything below $5 million plus a deductible based on their premium above that mark. Though neither private companies nor the government will pay for any damages over the $100 billion mark, industry representatives have already stated that insurers cannot absorb another 9/11 hit.

Another issue potentially created by TRIA is sited in several studies that show private insurance being crowded out by public assisted insurance programs creating various interrelated problems, such as forcing the public to pay a larger bill. There is also the risk that the shift will make private insurance markets less competitive or it will shrink the overall market. Both of these risks, if they become reality, will result in raised prices for consumers.

Boardman concludes that state mandated terrorism insurance is ultimately going to weaken the insurance industry and fail to meet targeted incentive effects which are aimed at making insurance preferable to entitlements. TRIA is scheduled to fully terminate by the end of December of this year and is currently up for renewal. However, regardless of whether the government decides to continue state mandated insurance, the public, via government, will monetarily relieve victims of the next terrorist act, just as federal funds were made available after 9/11. With the understanding that federal assistance is always going to be there in one form or another, the most cost effective way to provide it, according to Boardman, is through a direct payment approach. The direct payment approach is simply drawing funds from the Treasury Department to aid victims of terror attacks. The advantage of this approach is not only that the federal government will never declare bankruptcy, but it is cheaper, will preserve the insurance structure, and open the door for the possible creation and development of a private terrorism insurance market.

Michelle Boardman

The full article can be viewed in the March 2005 issue of the *Georgetown Law Journal*. ❖

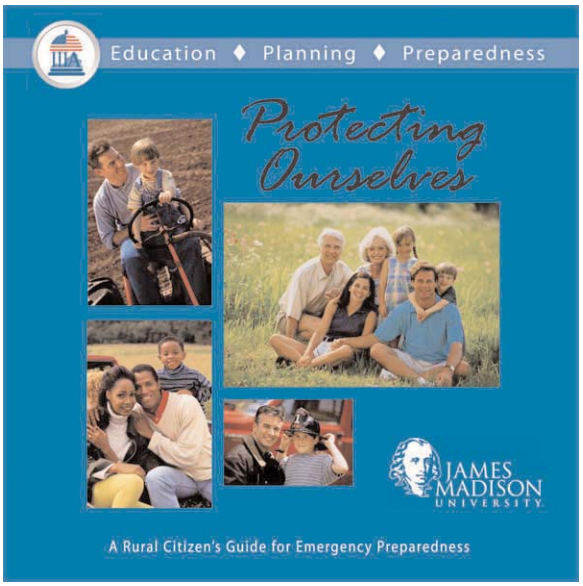
JMU Releases
Protecting Ourselves: A Rural Guide for Emergency Preparedness

Dr. John B. Noftsinger, Jr, Associate Vice President and Executive Director
Institute for Infrastructure and Information Assurance, James Madison University

The Institute for Infrastructure and Information Assurance (IIIA) at James Madison University recently published *Protecting Ourselves: A Rural Guide for Emergency Preparedness*. Unveiled in May at the 2005 IIIA Research Symposium, this guide offers a comprehensive analysis of the threats facing American communities and provides citizens with strategies to heighten personal protection and security.

Protecting Ourselves, the second edition IIIA Citizen's Guide, places a unique emphasis on rural populations and the emergencies that can impact these localities. Utilizing a framework centered upon education, planning, and preparedness, this text confronts topics such as natural disasters, technological failures, shelters and sheltering-in-place, information security, and evacuation. In addition, *Protecting Ourselves* integrates guidelines from government agencies such as the Federal Emergency Management Agency (FEMA) and the American Red Cross, with scholarly research, providing citizens with a wide range of pertinent information.

> ***Q. How do you prevent a panic response?***
>
> ***A. Prepare for emergency situations and practice your response plan.***



Furthermore, the guide offers a detailed examination of topics that are of vital importance to many individuals, but go largely unaddressed by contemporary literature. Specifically, *Protecting Ourselves* delves into the threats facing children, special needs populations, and livestock and pets, while also presenting useful tips to ensure the safety of these groups during times of crisis.

While this second edition Citizen's Guide focuses upon rural communities, the information provided is extremely relevant to all individuals, no matter where they may reside. Since natural disasters, terrorist attacks, and cyber crimes pose threats to society at large, the suggestions presented in this user-friendly text remain applicable to all. By examining *Protecting Ourselves* and taking measures such as establishing a family communications plan and preparing a home emergency kit, citizens are able to take the appropriate measures to increase their resiliency in emergency situations.

The strong partnership between the IIIA and George Mason University has fostered groundbreaking research within the field of homeland security. These efforts have allowed the Critical Infrastructure Protection Program to produce exceptional scholarly works, while also providing a valuable service to the general public. We are proud to introduce the latest publication, *Protecting Ourselves: A Rural Guide for Emergency Preparedness*. A copy of the Citizen's Guide can be downloaded from the IIIA website at: www.jmu.edu/iiia/news.html. ❖

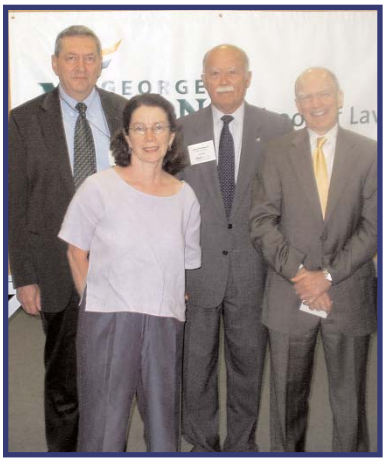
CIP Program Hosts Privacy Conference

Over one hundred people attended Distinguished Adjunct Professor of Law John O. Marsh and the Critical Infrastructure Protection Program's conference, *Privacy, Security and Technology in the 21st Century: Addressing the Legal Landscape of Today and Tomorrow.* The June 16th event examined the intersection of privacy and national security and the challenges facing the current and next generation of legal leadership.

During the workshop, speakers addressed the legal challenges in balancing privacy and security concerns in the context of the war on terror, ethical issues arising from the concept of privacy, and the impact of technologies and capabilities on privacy. Speakers and panelists included; Daniel Polsby, John A. McCarthy, Angeline Chen, Suzanne Spalding, Nancy Libin, Paul Rosenzweig, Jeremy Bash, Stewart Baker, M.E. Bowman, Kate Martin and John Poindexter.

The panelists and participants represented a diverse cross-section of privacy issue stakeholders, including government, private sector, academia, and non-profit organizations. The workshop included not only lively debate, but draft recommendations for the current and future leadership of our legal system.

The CIPP website will be updated to include biographies of panelists and the papers that were distributed at the conference. Please check back frequently at http://cipp.gmu.edu/.



Top: Professor Angie Chen and Secretary John Marsh with DHS Chief Privacy Officer, Nuala O'Connor Kelly.
Middle Left: Panel One speakers, Jeremy Bash, Nancy Libin, Suzanne Spaulding, and Paul Rosenzweig.
Middle Right: Panel Two speakers, M.E. Bowman, Kate Martin, John Poindexter, and Stewart Baker.
Bottom: Secretary John Marsh, John Poindexter, and John McCarthy

Business Case *(Cont. from Page 3)* participants that the establishment of mandatory, enforceable reliability standards was a critical component to not only improve reliability in the electricity sector, but also to better define insurance risk through improved data reporting and compliance monitoring. The use of insurance was also discussed as a market-based tool to promote reliability. Workshop participants debated the use of various market-based approaches such as variable levels of customer reliability and grid-friendly appliances to enhance bulk-electric system reliability. Customer purchased insurance could be applied to these techniques to optimize grid operation and responsiveness.

The CIP Program is currently preparing a summary of the workshop and a white paper on action items and future research to promote insurance products in the electric sector. These will become available in the next few months and will be made available through the CIPP web site. The research will be continued through a more thorough investigation of an expanded role for insurance, as well as other market based incentives for reducing risks and vulnerabilities within the complex electricity infrastructure. ❖

GAO Report: CATASTROPHE RISK

U.S. and European Approaches to Insure Natural Catastrophe and Terrorism Risks Released February 2005

Owing to the wide acknowledgement that natural catastrophes and terrorist attacks could burden the insurance industry with heavy financial pressures, resulting in higher premiums and reduced coverage, the Government Accountability Office (GAO) released a study overviewing the insurance industry's current capacity to cover natural catastrophic risk, analyzing the potential of catastrophe bonds and tax-deductible reserves to enhance private sector capacity and describing approaches taken by six European countries to address natural and terrorist catastrophe risk. The study found that despite steps in recent years to strengthen insurer capacity, no catastrophe event or series of events have tested these improvements. While the hurricanes that battered Florida in 2004 wreaked over $20 billion in damages, only one Florida insurance company failed, in contrast to the eleven that failed after Hurricane Andrew in 2001, owing to stronger building codes and stricter underwriting standards.

According to the GAO, catastrophic bonds, a type of security issued by insurers and reinsurers (companies that offer insurance to insurance companies) and sold to institutional investors, could be of benefit in diversifying the funding base for catastrophic risk, but currently only occupy a small piece of the global catastrophe reinsurance market and cost significantly more than traditional reinsurance. Furthermore, these bonds are not considered feasible by industry for terrorism risk at this time. The establishment of tax-deductible reserves for potential catastrophic events has been advanced to enhance industry capacity, but could lower federal tax receipts and may not bring the needed increase in capacity if insurers substitute the reserves for other types of capacity.

The study also examined approaches taken by six European countries to address catastrophic risk, ranging from governmental requirements for insurers to provide natural catastrophic insurance and financial assistance to insurers after catastrophic events, to a reliance upon the private market. Despite the varying approaches, insurers in all six countries were allowed to establish tax-deducible reserves for potential catastrophic events and the majority of these governments have established national terrorism insurance programs.

The complete GAO Report can be found at www.gao.gov/cgi-bin/getrpt?GAO-05-199. ❖

Information Risk *(Cont. from Page 6)* and property policies use the terms "physical damage" and "tangible property" to define the limits of a covered loss. The court decision thus confirmed what insurers were trying to achieve exclusion of e-business claims from traditional policies.

One of the main things insurers want to see is that your IT staff has patched known vulnerabilities, with special attention to the most critical ones.

In its ruling, the 4th Circuit compared the loss of data to the loss of a lock's combination: "When the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged. With the retrieval or resetting of the combination–the idea–the lock can be used again."[1] Such, said the court, is also the case when data is lost or software malfunctions. Numerous other court cases have likewise ruled that data is not tangible property, though there have been exceptions.[2]

Cyberrisk Insurance

Insurers have developed cyber risk policies to fill in the gaps left by exclusions in traditional policies. These policies can provide coverage for both direct loss to companies and liabilities . Insurers generally write these policies in modular form, so an organization can put together a policy that makes sense based on its unique information-risk profile.

Coverage is available for risks including:

- loss or corruption of electronic data, information, or computer resources and the costs to rebuild such data or information;
- business interruption/income loss and extra expenses, including revenue losses from a denial-of-service attack and the cost of implementing backup systems and IT security responses;
- systems related extortion;
- liability to others for loss of data or damage to their computer systems;
- liability for failure of professional service provided over the Internet;
- liability for content on your Web site or another organization's site;
- liability for Internet advertising offenses;
- liability for infringement of intellectual property; and
- liability resulting from network security beaches, such as disclosure of customer information.

Working With Insurers

In general, insurers look to make sure that the level of information security in place at a company is appropriate in relation to its size and its industry sector. For example, a multinational financial institution should have a much more sophisticated and deeper level of security than a retail operation with only a few outlets.

Insurers will want to view a company's IT security through the lens of a security framework, such as ISO 17799 to make sure it has the proper policies, procedures, and technical fixes in place. Some of them will want their own personnel to run the checks; others will interview the person in charge of an organization's IT security.

Many insurers will also insist on scanning your system with specialized software that probes for security holes. One of the main things insurers want to see is that your IT staff has patched known vulnerabilities, with special attention to the most critical ones.

The bottom line is: Be prepared to answer some detailed questions from underwriters regarding your information-security practices. One of the best ways to ensure your application is viewed in the best possible light is to go to the cyber insurance marketplace armed with solid documentation showing that your organization takes systems security seriously.❖

[1] *America Online, Inc. v. St. Paul Mercury Insurance Co.*, 347 F.3d 89 (4th Cir. 2003).
[2] For example, see an Arizona case, *American Guarantee & Liability Insurance Co. v. Ingram Micro Inc.*, Civ. 99-185 TUC ACM. In this case, a lower court ruled that a power outage that caused a firm to lose the use and functionality of its computers did constitute "direct physical loss or damage" under its insurance policy. A higher court declined to accept American Guarantee's appeal.


Dr. Ken Friedman

DOE *(Cont. from Page 4)* from these storms. The Edison report also points out that there is little consistency in establishing which events qualify for special accounting treatment for disaster recovery and restoration costs.

"Self-insurance" is only one possible approach to preparing for natural catastrophe and terrorism risks. Commercial insurance, if it were to become financially feasible, might provide another means to expedite cost recovery for the utilities. The U.S. General Accountability Office has produced a report "Catastrophic Risk: U.S. and European Approaches to Insure Natural Catastrophe and Terrorism Risks," (2005) which examines approaches currently being used and points out that the lack of affordable insurance coverage in the marketplace could impede economic recovery and development.

The current work at GMU will provide needed insights into the role of insurance in securing the Nation's energy infrastructure. Ultimately, creative use of insurance and underwriting standards may help reduce the psychological and economic consequences to the U.S. of future events. The results of this collaborative effort will provide an important framework for DOE in its ongoing programs in energy assurance. ❖

TRIA Renewal *(Cont. from Page 2)* program certain lines of insurance that are less subject to aggregation risks and should be left to the private market. Treasury Secretary John W. Snow stated, "It is our view that continuation of the program in its current form is likely to hinder the further development of the insurance market by crowding out innovation and capacity building."

Where do we go from here?

As the TRIA debate continues, these are some of the questions that are steering the discussion:
1) In the long-term, which entity can best determine the necessity for, and extent of terrorism insurance? Market mechanisms or the government?
2) If market forces are the answer, is TRIA still needed as a transition vehicle? Is another mechanism required? Or should the government remove itself from the equation altogether?
3) If government assistance is the answer, should it play a temporary or permanent role? ❖

How Andrew Changed Storm Insurance

Until Hurricane Andrew in 1992, commercial insurance was widely available at affordable rates to protect against catastrophic storms. FPL, for example, had a transmission and distribution policy with a limit of $350 million per occurrence. The 1992 premium for this policy was $3.5 million. After Hurricane Andrew, commercial insurance carriers stopped writing such policies altogether or made them so expensive that they could not be justified. For example, the quote FPL received in 1993, the year after Hurricane Andrew, was for $23 million for a transmission and distribution system policy with an aggregate annual loss of $100 million.

In lieu of paying for expensive storm insurance, FPL elected to self-insure. It currently funds its storm reserve account at a level of about $20 million a year. This amounts to about 20 cents per month for a typical residential customer.

From *After the Disaster: Utility Restoration Cost Recovery*, Edison Electric Institute

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://techcenter.gmu.edu/programs/cipp/cip_report.html.