

Pennsylvania House Veterans Affairs and Emergency Preparedness Public Hearing



Cyber-Terrorism:
The Security of Banking, Financial and Insurance Systems

Thursday, October 16, 2003

Pennsylvania Insurance Department
Commonwealth of Pennsylvania

**PENNSYLVANIA INSURANCE DEPARTMENT TESTIMONY PRESENTED
TO THE PENNSYLVANIA HOUSE VETERANS AFFAIRS & EMERGENCY
PREPAREDNESS**

Is insurance the first thing a person thinks about when contemplating the potential fall-out from cyber-terrorism? Well, probably not.

But when you consider that cyber-terrorism can be used as a fairly broad and comprehensive way to achieve terrorist objectives, as well as to wreak complete havoc in the marketplace, the insurance view comes more clearly into focus.

It may be helpful for purposes of today's discussion to focus on the following three areas:

- The risk exposure of the insurance industry to cyber-terrorism;
- The potential impact of cyber-terrorism events upon insurers responding to other disasters;
- The need for cyber-risk insurance coverages for the overall business population.

If we are to truly secure, our economy, the government and the insurance industry's ability to respond to disaster must be partnered with business's ability to buy coverage, prevent or mitigate loss and otherwise care for itself first and foremost.

The need for society to invest in cyber-security cannot be overstated. However, regardless of the amount of resources expended by individuals, businesses and government in this endeavour, our nation can never be fully protected against hackers and cyber-terrorists who are continually seeking to exploit vulnerabilities in newly developed security systems.

Insurance coverage plays an essential part in protecting businesses against the financial consequences of a cyber-attack that defeats the implemented cyber-safety measures. By developing appropriate products that allow individuals and businesses to transfer the retained risk of a cyber-attack, the insurance industry can play a vital role in protecting our nation's cyber-infrastructure.

According to estimates from PricewaterhouseCoopers, the total worldwide business losses from the various collateral effects of cyber-attacks totalled \$1.5 trillion in the year 2000 alone.

In the United States, there are a number of public/private initiatives developed in the face of the growing threat of cyber-terrorism perpetrated both by groups and individuals.

But risk managers have to see they are buying suitable protection. Traditional non-commercial property/ casualty policies do not provide coverage for losses stemming from a cyber-attack. There generally has to be some kind of physical damage before a conventional property policy is triggered. Since a cyber-attack will not, in all likelihood, result in physical damage, a majority of the resultant losses will not be covered by the typical property policy.

Businesses concerned about their cyber-risk exposure do have access to tailored cyber-risk coverage that can address the specific technology utilized and unique risk levels faced by the insured. On a first-party basis, such policies will often cover corruption of data and business interruption losses stemming from a cyber-attack, and can also provide recompense to insureds for the repair or reconstruction of servers and websites, as well as reconstruction of lost data.

Some policies will even provide for third-party liability coverage for claims arising out of the cyber-attack. However, while these policies do exist, it remains a relatively new market, served by only a handful of insurers. You may find some of these policies are issued primarily in the surplus lines marketplace – if at all.

The reason for this may be the challenges for insurers looking to offer cyber-protection policies due to the limited loss data available to appropriately price the product. Data has to be “mature” – meaning it has to have developed over a period of years – relying on more than one event.

According to a recent Ernst & Young survey of 1,400 organizations in its 2003 Global Information Security Survey, only seven percent of respondents knew they had a specific insurance policy geared to this network and cyber-risk. Nearly a third (33 percent) thought they had coverage they actually lacked. Another 34 percent knew they lacked such coverage, while 22 percent didn't know the answer. Ernst & Young characterized the fact that only 7 percent of surveyed companies had cyber insurance as “astonishingly low, given the risk environment and the fact that general policies don't provide such coverage.”

Regardless of its product line or service, virtually all major businesses today rely on computer networks to function. They need to recognize, however, that network security risks are fundamentally different than traditional physical risks like fire. If a hacker or virus shuts down a network or destroys computer software or data, most businesses today have either

limited or no coverage. Insurers have excluded these risks from standard commercial policies and are now offering stand-alone coverage. Whether your company conducts business over the Internet, stores customer data on servers or simply uses email, it is at risk.

Risk is at the heart of nearly every business, personal, and governmental decision made these days—from the risks of business travel to decisions involving foreign investments or sports teams visiting cities where terrorist threats or health risks exist. Risk is headlined on the front pages of our daily newspapers and in nearly every television broadcast. It colors the decision-making process in everything from school trips to our nation's capital, to the family vacation destination.

Assessing risk – looking at the exposure – is what insurance companies do. That is part of their job and inherently part of an insurer's nature.

Now is the time for risk managers and insurance professionals to step forward and help address some of these risks in a more logical and professional manner. Often, simple risk management solutions can yield surprising results and assist in a logical decision-making process. The time-proven approaches of risk identification, risk analysis, evaluation, control, financing, and administration still apply. Coupled with risk management techniques focused on avoidance, prevention, reduction, transfer, and

financing, large corporations and small concerns alike can craft better decisions and allocate resources more efficiently to counter actual risk.

Businesses are more likely to be attacked than government or military facilities. According to data from the U.S. Department of State, a total of 2,784 terrorist attacks were made from 1996 to 2001 against business, diplomatic, government, military, and other facilities across the globe. Of these, more than 1,902 attacks were made against businesses, while the total for government organizations, including diplomatic facilities and military installations, accounted for only 335 of the almost 2,800 attacks during that same period. Government targets accounted for only 12% of the total.

Clearly, the loss data suggest that business targets are 21 times more likely to be struck than government facilities; 39 times more likely than military targets to be attacked; and nearly 10 times more likely to be targeted than embassies, consulates, and legations.

This is something else insurers look at – frequency – how often something has occurred and the likelihood of it occurring again. The frequency rates for attacks against business offices and facilities are increasing at very rapid and alarming rates, which may continue, if not increase, in the future.

Local insurance agents, brokers, risk managers and consultants can be of vital assistance to not only their clients, but also to local civic groups and organizations faced with making risk-based decisions in an uncertain and more often dangerous world. Who better in your community understands the concepts of risk and risk-based decision-making? Whether it may be a client with international operations or the local school board deciding upon the wisdom of an exchange concert, a foreign trip planned by a seniors' group or a European vacation being considered by an important client, these individuals contribute in very meaningful ways to assist people in understanding relative risk and to help in some reasonable degree to better manage risk.

Certainly, our world prior to the events of September 11 is distinctly different than our world from that point in time on. The world stopped for all of us, and a new world was born. That is certainly true in the insurance industry.

The immediate insurance market response to September 11 was one of shock, but not one of panic. Now, as we have progressed beyond the shock, we have seen the insurance marketplace settle down and beginning looking at insurance in the face of what had been previously unseen or unknown in terms of risk exposures.

Property, casualty, life, health, accidental death and disability, workers compensation, aviation, auto insurance and reinsurance were called upon to pay tremendous losses.

The challenges we now face were unimaginable three years ago at this time. If you examine the record of the Pennsylvania Insurance Department during this period, you would find that the Department has been willing and able to take on many challenges. The Department's charge was, and is, to make Pennsylvania a better marketplace for insurance consumers increasingly facing more complex and life changing decisions. We know that insurance consumers are your constituents. That is why the Department has seen the insurance industry as a partner, not an adversary, in creating a sound regulatory environment.

As you know, the best marketplace for the insurance consumer is one that recognizes the importance of having as many quality products available as possible, offered by carriers that are financially viable, and sold by producers who are committed to marketing the types of products that meet consumer needs.

Following the terrorist attacks of September 11, 2002, there was much uncertainty in the markets for commercial lines property and casualty insurance coverage in light of sustained losses. In particular, many reinsurers announced that they had no intention of providing coverage for acts of terrorism in future reinsurance contracts. As such, interested parties sought a temporary federal backstop to calm market fears over future terrorist attacks.

On November 26, 2002, the President signed the Terrorism Risk Insurance Act of 2002 (“Act”). The purpose of the Act was to create a temporary federal program, which may be extended, under which the federal government would share the risk of loss from future terrorist attacks with the insurance industry. The Act imposed certain obligations on insurers.

Under the Act, the federal government will step in and cover claims for acts of terrorism in excess of \$5 million. An “act of terrorism” is defined by the Act as any act that is certified by the Secretary of Treasury, in concurrence with the Secretary of State and the Attorney General of the United States

- (i) to be an act of terrorism;
- (ii) to be a violent act or an act that is dangerous to
 - (I) human life;
 - (II) property; or
 - (III) infrastructure;
- (iii) to have resulted in damage within the United States, or outside the United States in the case of
 - (I) an air carrier or vessel described in paragraph (5)(B) of the act; or
 - (II) the premises of a United States mission; and
- (iv) to have been committed by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian populations of the United States or to influence the policy or affect the conduct of the United States Government by coercion.”

Insured losses covered by the Act include losses under primary property and casualty insurance for commercial lines, workers’ compensation and surety.

The Department’s Office of Chief Counsel worked very closely with the NAIC Catastrophe Insurance Working Group, prior to November 26, 2003, to develop a model bulletin and disclosure forms as required under the Act. The purpose of the bulletin was to advise insurers of certain provisions of the Act that may require insurers to submit a filing in this Commonwealth and to inform insurers regarding a voluntary procedure for insureds to use to expedite the filing and timely review of disclosure notices to policyholders, policy language and the applicable rates that are discussed in the Act. The NAIC model bulletin was revised to satisfy Pennsylvania specific issues and was published on the Department’s web site on November 26, 2003. (A copy of the bulletin is attached to this testimony.)

Publication of this bulletin was a great achievement for the Department, as it provided the industry with ready, easily understood directions for complying with this complicated Act.

As the Terrorism Risk Insurance Act approaches its first anniversary, demand for terrorism insurance is low, but the backstop is bringing capacity and stability to the marketplace. It may not be a “popular” product, but the fact that it is available at all is a sign that the Terrorism Risk Insurance Act of 2002 has been successful. But, we must be cognizant that this is just a temporary fix – the act is slated to expire in 2005.

Even with the backstop in place, insurers still have considerable risk. Businesses can reduce their cost for terrorism insurance by taking actions to decrease their vulnerability or exposure to risk. The average American business is not the World Trade Center. All businesses can limit access to their facilities and take steps to make the facilities themselves safer.

Our world IS different than it was three years ago. That is simple, unalterable fact. Looking at all the risk exposures going forward is the insurance industry’s job. It is important to understand and reduce the risk.

Thank you for providing the Department the opportunity to submit written testimony on this important topic. Should you have any questions, please do not hesitate to contact Lesa Tressler in the Department’s Office of Legislative Affairs.